Q1 2024 Threat Landscape Report

nuspire

Surge in Ransomware, Dark Web Commerce and Exploit Activity

nuspire.com

```
import os, json, uuid, time
from datetime import datetime

from flask import Flask, render_template, request, Response, redirect, url_for, send_file, jsonify
from flask_cors import CORS
import requests
from requests.auth import HTTPBasicAuth
from psycopg2_contextmanager import database_connection
import boto3

from auth import login_required

app = Flask(__name__)
app.config.from_object('config')
CORS(app)

lambda_client = boto3.client('lambda', region_name='us-east-1')

GS_API_URL = os.environ['GS_API_URL']
DATABASE_URL = os.environ['DATABASE_URL']
JOB_INGESTION_LAMBDA_NAME = os.environ['JOB_INGESTION_LAMBDA_NAME']


@app.route('/')
def serve_react_app():
    return render_template('index.html')

@app.route('/login', methods=['POST'])
def login():
    request_json = request.get_json()
    email = request_json.get('email')
    password = request_json.get('password')
    api_auth_endpoint = '{}v1/auth/'.format(GS_API_URL)
    auth_response = requests.get(api_auth_endpoint, auth=HTTPBasicAuth(email, password))
    excluded_headers = ['content-encoding', 'content-length', 'transfer-encoding', 'connection', 'www-
    auth_response_headers = [(name, value) for (name, value) in auth_response.raw.headers.items() if n
```

This report is sourced from **over a trillion traffic logs** ingested from Nuspire client sites and associated with thousands of devices around the globe.

nuspire

What's in the Report

Introduction:

Diving deeper into ransomware, dark web and vulnerability exploits

As the first quarter ends and we usher in a new year, it's crucial for us to adapt and evolve our reporting to keep pace with the rapidly changing threat landscape. The analysis of our recent report data and trends clearly indicates the necessity for us to deepen our analysis of ransomware, dark web and exploit activities. This focused approach will enable us to comprehensively address the spectrum of threats organizations face and devise more robust strategies to counter these escalating cybersecurity challenges.

Ransomware Publications

Dark Web Listings

Exploits

Q1 2024 Summary of Findings

11,789,860 total

Q1 Exploitation Events

52.61%

increase in total activity from Q4

1,601 total

Q1 Ransomware Publications

3.69%

increase in publications from Q4

3,938,507 total

Q1 Dark Web Marketplace Listings

58.16%

increase in total listings from Q4

How We Crunch the Numbers

Nuspire's Threat Intelligence Team follows a five-step the following five-step data analysis methodology.

GATHER

Nuspire sources threat intelligence and data from global sources, client devices and reputable third parties.

1

PROCESS

Data is analyzed by a combination of machine learning, algorithm scoring and anomaly detection.

2

DETECT

Log data is ingested using Nuspire's cloud-based SIEM, which alerts the security operations center (SOC). The SOC then notifies the client and works with them to remediate the threat.

3

EVALUATE

Analysts further scrutinize the research, scoring and tracking of existing and new threats.

4

DISSEMINATE

Analysts leverage the insights to constantly improve the SOC, alerting the community through the creation of detection rules, briefs and presentations.

5

Malware

Detection, Q2 2023

Across Nuspire-managed and monitored devices, there was a decrease of 45.51% in total malware activity compared to Q1 2023

How to Combat

To strengthen your defenses against malware activity, you'll need to adopt a multiprong approach including endpoint protection platforms and cyber awareness training.

Q1's Top Threat Events

January 3
Infostealers Abuse Google OAuth Endpoint to 'Revive' Cookies, Hijack Accounts

January 4
Researchers Release Decryptor for BlackBasta Ransomware

January 10
Microsoft's January Patch Tuesday Addresses 49 Vulnerabilities, Including Two Critical

January 17
Over 178K SonicWall Firewalls Vulnerable to DoS, Potential RCE Attacks

January 18
FBI and CISA Warn of Androxgh0st Malware Attacks

January 23
CISA Emergency Directive Demands Action on Ivanti Zero-Day Vulnerabilities

January 24
Critical VMware vCenter Vulnerability Exploited in the Wild

January 31
New Ivanti Connect Secure Zero-Day Exploited by Threat Actors

February 6
Ivanti Connect Secure Zero-Day Now Under Mass Exploitation

February 7
Critical Cisco Vulnerability Allows CSRF Attacks on Express Series Gateways

February 9
New Fortinet RCE Vulnerability Announced for SSL-VPN

February 9
Critical Format String Bug Announced by Fortinet Affecting FGFM Daemon

February 14
Microsoft's February Patch Tuesday Addresses 2 Zero-Days, 73 Vulnerabilities

February 15
Zoom Announces Critical Vulnerability for Desktop Application

February 19
SolarWinds Fixes RCE Vulnerabilities in SolarWinds ARM Products

February 20
Law Enforcement Seize LockBit Servers and Arrest Operators in Global Operation

February 20
ConnectWise Announces Critical Vulnerabilities Affecting ScreenConnect

February 23
UnitedHealth's Optum Attacked, Causing U.S. Healthcare Billing Outages

March 5
Critical Vulnerability Announced in JetBrains' TeamCity with Exploit Available

March 13
Microsoft's March Patch Tuesday: Two Critical Security Updates Released

March 21
CISA, NSA, FBI and Five Eyes Issue New Alert on Chinese APT Volt Typhoon

March 27
CISA Warns of Active Exploitation of Flaws in Fortinet, Ivanti & Nice Linear

Q1 2024

1,601 Total Ransomware Extortion Publications

133

publications averaged per week

19

publications averaged per day

3.69%

increase in publications from Q4

Ransomware

LockBit Remains Prevalent Despite Law Enforcement Disruption

Figure 1 shows the average Q1 ransomware extortion publication activity in a dashed trend line. Nuspire monitors known ransomware operators' extortion sites where, following a successful attack, these gangs will attempt to extort the victim into paying their ransom by threatening to release stolen data if not paid.

The solid line shows the true weekly numbers to help identify spikes and abnormal activity. In comparison to the fourth quarter, publications on ransomware extortion have risen by **3.69%**, indicating that ransomware operations remain unaffected by recent law enforcement efforts and are, in fact, on the rise. Ransomware and its financially motivated threat actors remain among the top threats to organizations worldwide.

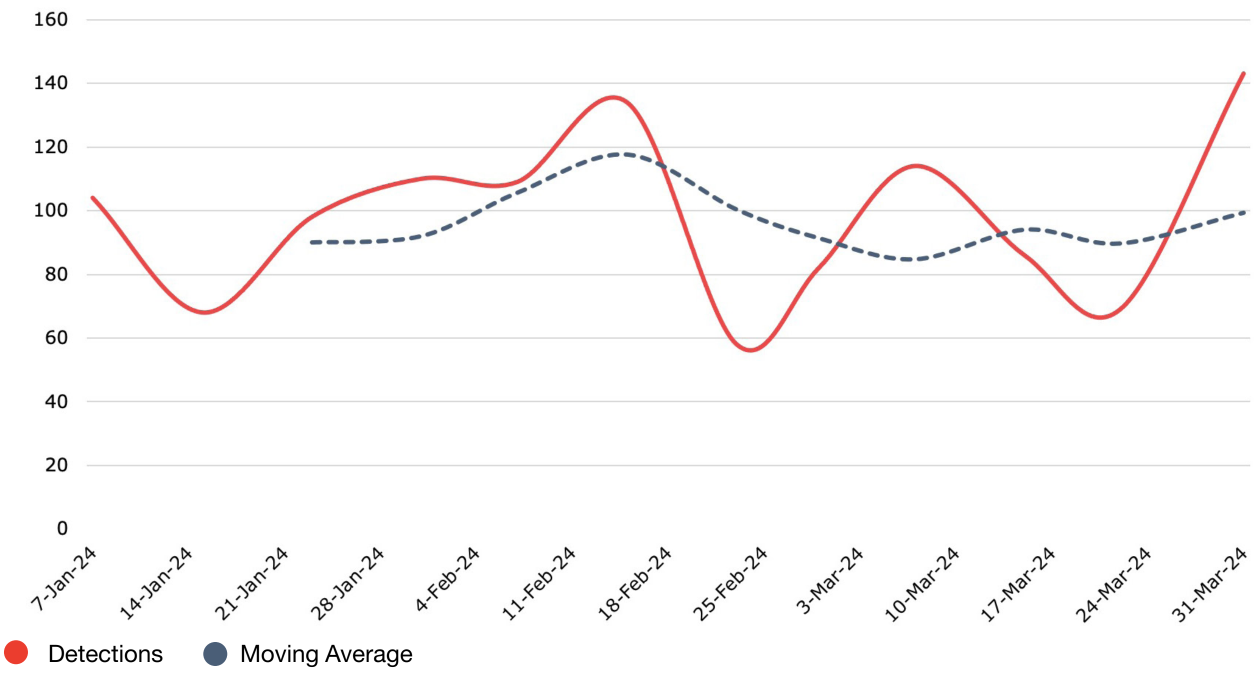


FIGURE 1. RANSOMWARE EXTORTION PUBLICATIONS | NUSPIRE, Q1 2024

As shown in Figure 2, the top ransomware operator witnessed throughout Q1 was LockBit. On Feb. 20, 2024, The U.S. Department of Justice announced, through a joint operation, that it had disrupted LockBit's operations. Subsequently, LockBit's publications saw a sharp drop on its extortion site; however, the temporary downturn in LockBit's extortion publications was short-lived, as we witnessed a rapid recovery, reflecting the group's resilience and adaptability. Activity continued into the end of the quarter, and even with the disruption, extortion publications still increased by **1.74%** compared to Q4.

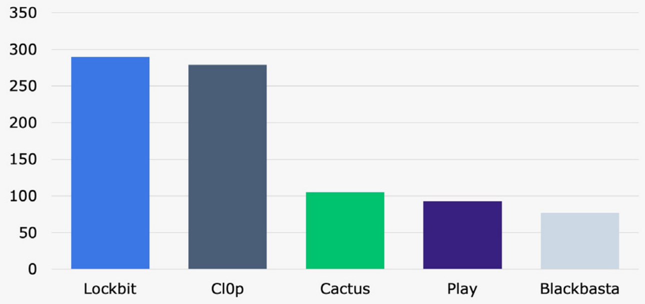


FIGURE 2. TOP FIVE RANSOMWARE OPERATORS
NUSPIRE, Q1 2024

Ransomware

LockBit Ransomware Ecosystem: Affiliate Dynamics and Revenue Distribution

As LockBit is affiliate-based and a ransomware-as-a-service (RaaS), any threat actor can "sign up" to use its ransomware toolkit and control panel. In return, LockBit collects a portion of the ransom payments affiliates receive from their victims.

Adversaries use a variety of attack vectors, often tailored to the individual threat actor's skills and preferences. Below are some of the most witnessed vulnerabilities and tools, as well as common tactics, techniques and procedures (TTPs); however, it's important to note that this isn't an exhaustive list.

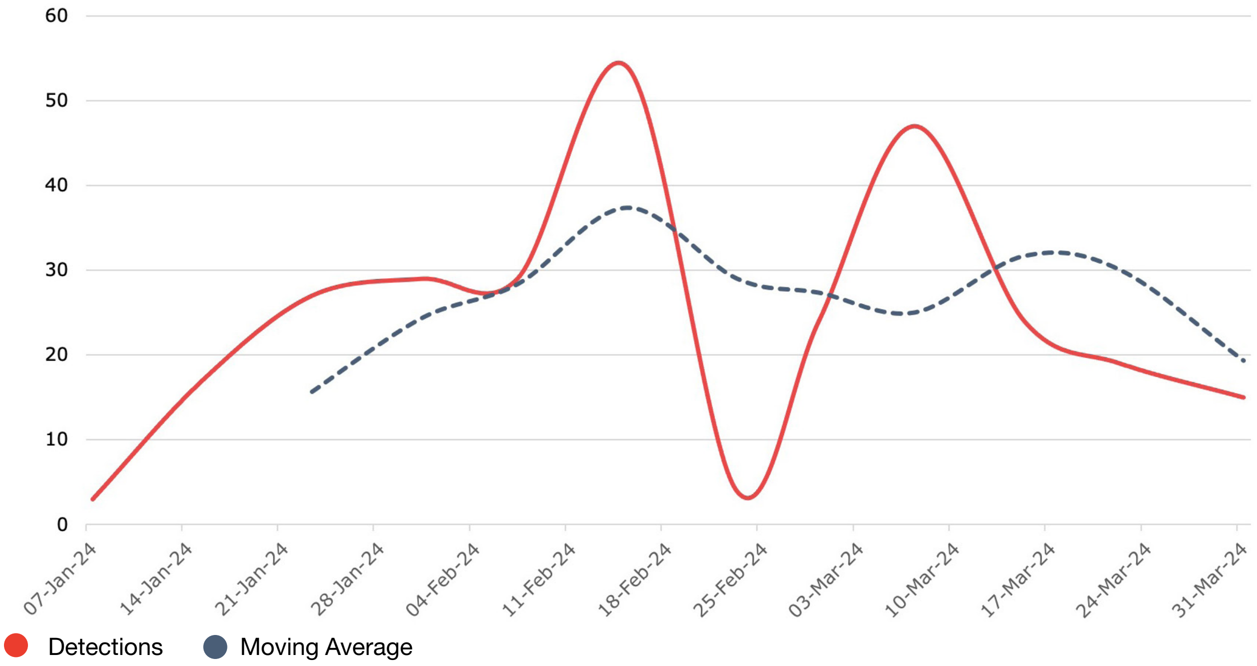


FIGURE 3. LOCKBIT EXTORTION PUBLICATION ACTIVITY | NUSPIRE, Q1 2024

Commonly Abused Vulnerabilities

CVE-2024-1709 – ConnectWise ScreenConnect Authentication Bypass

CVE-2024-1708 – ConnectWise ScreenConnect Path Traversal

CVE-2023-0669 – Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution

CVE-2023-27350 – PaperCut MF/NG Improper Access Control

CVE-2021-44228 – Apache Log4j2 Remote Code Execution

CVE-2021-22986 – F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution

CVE-2020-1472 – NetLogon Privilege Escalation

CVE-2019-0708 – Microsoft Remote Desktop Services Remote Code Execution

CVE-2018-13379 – Fortinet FortiOS SSL-VPN Path Traversal

Common Tactics, Techniques & Procedures (TTPs) for LockBit Ransomware

INITIAL ACCESS	
Drive-by Compromise	T1189
Exploit Public-Facing Application	T1190
External Remote Services	T1133
Phishing	T1566
Valid Accounts	T1078
EXECUTION	
Command and Scripting Interpreter: Windows Command Shell	T1059.003
Software Deployment Tools	T1072
System Services: Service Execution	T1569.002
PERSISTENCE	
Boot or Logon Autostart Execution	T1547
Valid Accounts	T1078
PRIVILEGE ESCALATION	
Abuse Elevation Control Mechanism	T1548
Boot or Logon Autostart Execution	T1547
Domain Policy Modification: Group Policy Modification	T1484.001
Valid Accounts	T1078
DEFENSE EVASION	
Execution Guardrails: Environmental Keying	T1480.001
Impair Defenses: Disable or Modify Tools	T1562.001
Indicator Removal: Clear Windows Event Logs	T1070.001
Indicator Removal: File Deletion	T1070.004
Obfuscated Files or Information	T1027
Obfuscated Files or Information: Software Packing	T1027.002
CREDENTIAL ACCESS	
Brute Force	T1110
Credentials from Password Stores: Credentials from Web Browsers	T1555.003
OS Credential Dumping	T1003
OS Credential Dumping: LSASS Memory	T1003.001
DISCOVERY	
Network Service Discovery	T1046
System Information Discovery	T1082
System Location Discovery: System Language Discovery	T1614.001
LATERAL MOVEMENT	
Remote Services: Remote Desktop Protocol	T1021.001
Remote Services: Server Message Block (SMB)/Admin Windows Shares	T1021.002

Common Tactics, Techniques & Procedures (TTPs) for LockBit Ransomware Cont.

COLLECTION	
Archive Collected Data: Archive via Utility	T1560.001
COMMAND & CONTROL	
Application Layer Protocol: File Transfer Protocols	T1071.002
Application Layer Protocol: Web Protocols	T1071.001
Non-Application Layer Protocol	T1095
Protocol Tunneling	T1572
Remote Access Software	T1219
EXFILTRATION	
Exfiltration Over Web Service	T1567
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
IMPACT	
Data Destruction	T1485
Data Encrypted for Impact	T1486
Defacement: Internal Defacement	T1491.001
Inhibit System Recovery	T1490
Service Stop	T1489

Ransomware

Sector Spotlight: The Manufacturing Industry's Battle Against Ransomware

In Q1, Nuspire observed a surge in ransomware attacks targeting the manufacturing sector, with LockBit and CL0P ransomware groups leading the charge. Given their pivotal role in supply chains, manufacturers represent lucrative targets for cybercriminals. The significant operational disruptions and consequent financial losses make manufacturers particularly vulnerable to ransom demands, often compelling them to acquiesce to attackers' demands more rapidly than other sectors.

The manufacturing industry also often has complex information technology (IT) and operational technology (OT) systems, and securing the interfaces between these systems can be challenging for these organizations. The increased technology and digitization of assets like IoT devices increase their attack surface and potentially introduce new vulnerabilities.

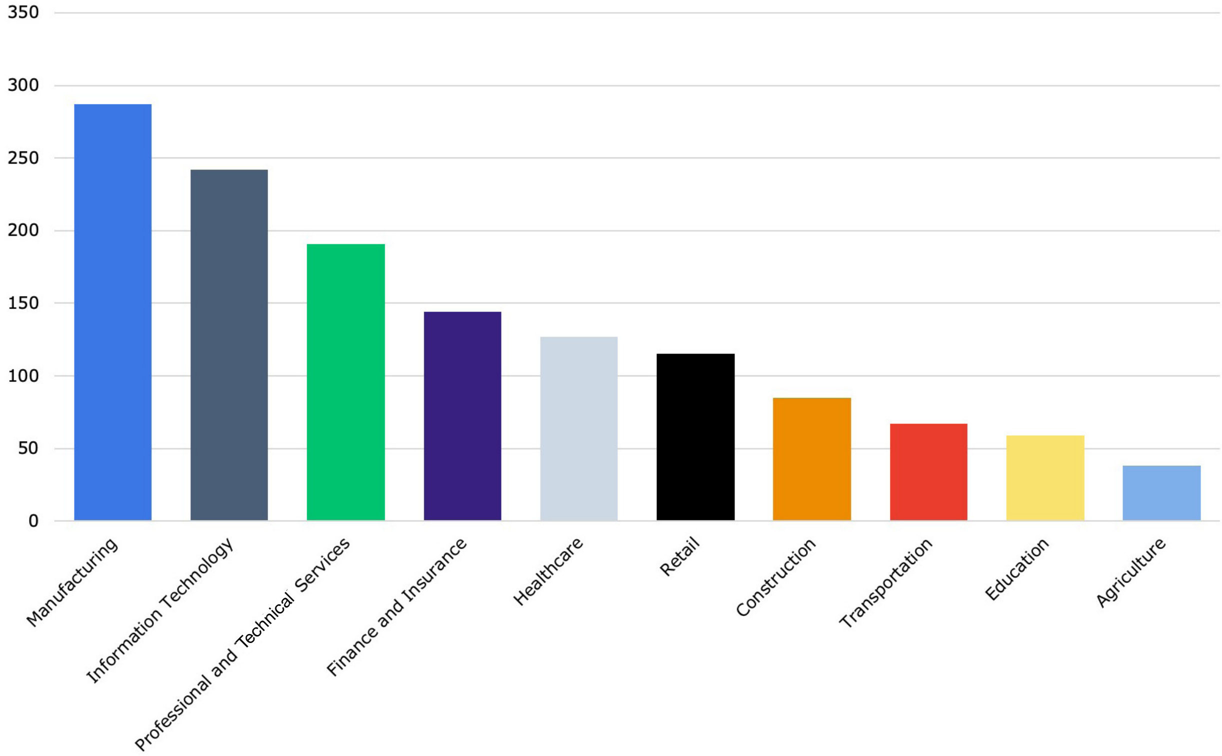


FIGURE 4. RANSOMWARE EXTORTION PUBLICATIONS BY INDUSTRY | NUSPIRE, Q1 2024

Historically, some manufacturing sectors haven't prioritized cybersecurity to the same extent as other industries, often because any changes to operations may result in downtime. This lack of investment and preparedness can make manufacturers easier targets for these ransomware operators. Additionally, manufacturers possess valuable intellectual property, including proprietary processes and patents, extending beyond ransom payments' immediate financial impact. This intellectual capital can be a lucrative commodity for cybercriminals to sell to the highest bidder.

Ways to Combat These Threats

Ransomware threats are constantly evolving using various tactics like phishing to exploit vulnerable systems. Addressing these threats necessitates a strategic approach focused on preemptive measures, advanced technological defenses and informed human behavior.

Endpoint detection and response (EDR)

EDR systems not only help prevent malware attacks through advanced threat detection mechanisms, but also offer detailed forensic capabilities and automated response actions to isolate infected endpoints and prevent the spread of ransomware. This approach ensures prevention as well as effective management of threats that penetrate the initial defenses.

Data backup and recovery plan

Organizations should implement robust, regularly updated and securely stored backups. This practice enables organizations to recover critical data without paying the ransom in the event of an attack. Backups should be encrypted, stored off-site or stored in a cloud service that is not directly accessible from the network to protect them from being compromised.

Cybersecurity awareness

Regular, engaging and comprehensive cybersecurity awareness training is essential for all employees. It should include simulated phishing exercises, updates on the latest cyber threat tactics and clear instructions on what to do if a potential security threat is detected. It is crucial that a security-focused culture is created within your organization.

Q1 2024 Dark Web Events

3,938,507 Total Marketplace Listings

437,657

listings of credit cards for sale

122,839

listings of email account access for sale

92,718

listings of social security numbers for sale

40,144

listings of shell access for sale

37,169

listings of RDP access for sale

13,606

listings of stolen accounts for sale

58.16%

increase in total listings from Q4

Dark Web

Monitoring Marketplace Trends and Infostealer Activity in Q1

Nuspire regularly monitors dark web marketplaces, a type of online forum or platform that operates on a part of the internet that is not indexed by traditional search engines. These marketplaces require special configurations and often special authorization to access. By monitoring this activity, Nuspire can determine trends in marketplace sales and what type of information-stealing malware (infostealers) is most commonly used by threat actors.

The dotted line in Figure 5 graphically represents the moving average of dark web marketplace postings for sale during the first quarter. It should be noted that a single posting may contain multiple entities and may not fully capture the depth of the data sold as much as showing how active the marketplaces are.

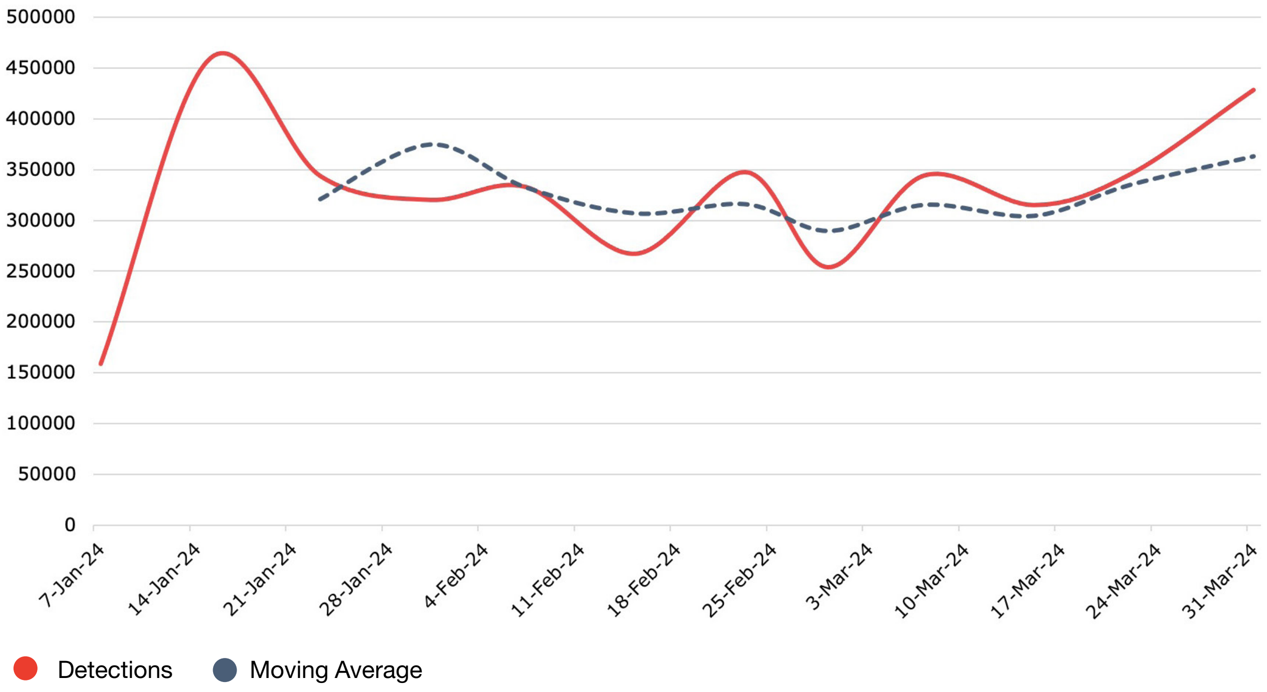
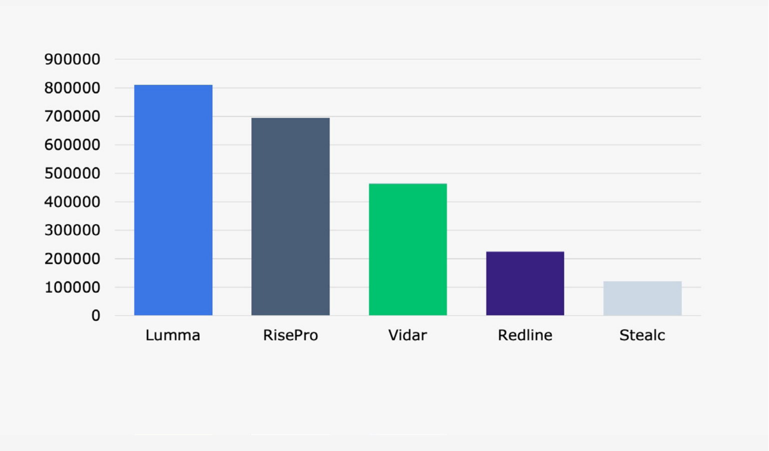


FIGURE 5. DARK WEB MARKETPLACE ACTIVITY Q1 | NUSPIRE, Q1 2024



Data on dark web marketplaces often comes from breaches or infostealer malware. Figure 6 shows the top five infostealers that harvest data from victim machines according to their marketplace listings. This information can help guide threat hunting activities and identify common deployment techniques that can be used in cybersecurity awareness training.

FIGURE 6. TOP FIVE INFOSTEALERS | NUSPIRE, Q1 2024

Dark Web

Lumma Stealer Activity More Than Doubles

Dark web marketplace listings using Lumma Stealer **more than doubled** compared to Q4 2023. Figure 7 shows the average Q1 Lumma Stealer activity in a dashed trend line. It first emerged in 2023 and quickly defined itself as a leader in infostealing malware. Lumma's developers advertise the malware on dark web forums and private access chats, offering developers a range of payment plans for use.

Lumma is spread through many common vectors seen with malware in general. It is often deployed through phishing emails, cracked pirated software or social engineering in chats like Discord and Telegram. Once installed, it checks if it is within a virtual environment with thorough anti-sandbox techniques. If Lumma determines it is not operating in a virtual environment, it shifts into its main mode, where it begins stealing information. It first reaches out to its command-and-control server to inform it of the new infection through an HTTP POST message. After establishing a connection, it begins to scan the system for files related to cryptocurrency wallets, browser profiles, persistent cookies and extensions from which it can steal data. Any data found is then transferred to the command-and-control server for exfiltration.

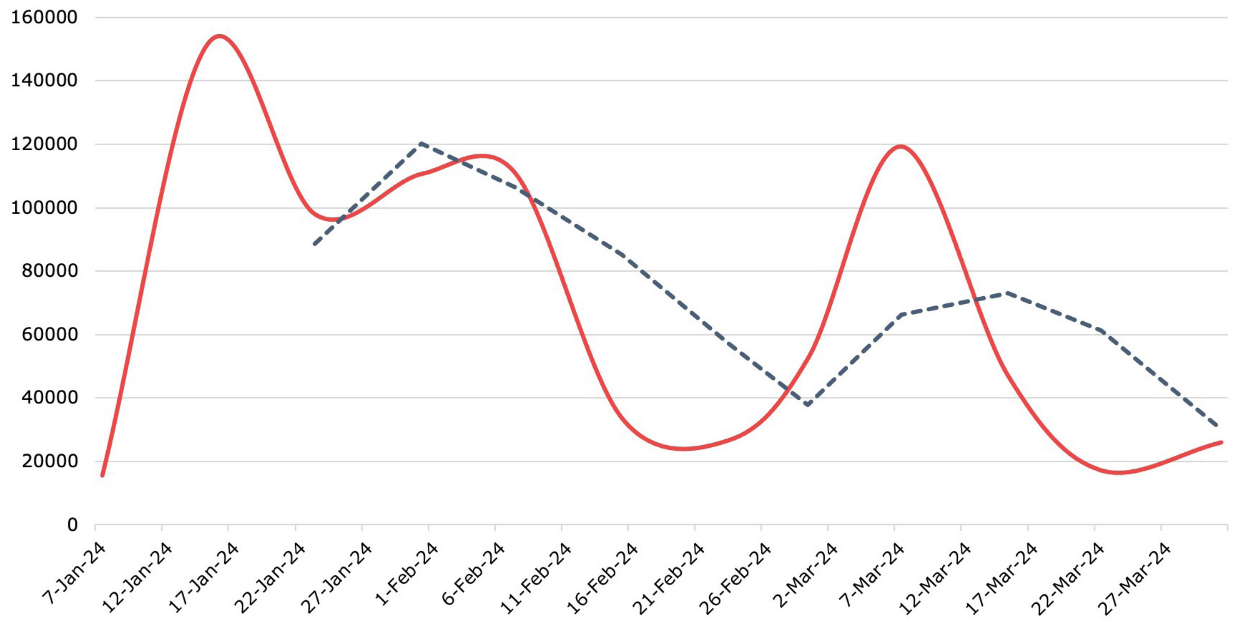


FIGURE 7. LUMMA STEALER ACTIVITY | NUSPIRE, Q1 2024

Ways to Combat These Threats

Data sales on the dark web and the threat of infostealer malware require proactive and robust security measures.

Implement comprehensive cybersecurity measures

Strengthen your defenses against infostealer malware by employing a layered cybersecurity strategy. This should include the use of advanced antivirus solutions that utilize machine learning and behavioral analysis to detect and block malware before it can exfiltrate data. Employ firewalls, secure web gateways and email security solutions to filter out malicious traffic and phishing attempts. Regularly update and patch all software to close vulnerabilities that attackers could exploit.

Enhance data protection and privacy

To prevent sensitive information from being sold on the dark web, it's crucial to minimize the amount of data shared online and ensure that the data is encrypted. Use end-to-end encrypted messaging services for sensitive communications and enable encryption on all devices. Additionally, employ strong, unique passwords for all accounts, complemented by multi-factor authentication (MFA), to add an extra layer of security. Consider using a reputable password manager to securely store and manage your passwords.

Educate and train on phishing and social engineering attacks

Since many infostealer malware infections originate from phishing or social engineering tactics, educating yourself and your organization's users about recognizing and responding to these threats is vital. Conduct regular training sessions that include the latest phishing techniques and provide clear guidelines on what to do if a suspicious email or message is received. Simulated phishing exercises can also help users practice their response to attempted attacks, thereby reducing the likelihood of successful infections.

Q1 2024 Exploitation Events

11,789,860 Total

360

unique exploits detected

982,488

exploits detected per week

140,355

exploits detected per day

52.61%

increase in total activity from Q4

Exploits

Hikvision Camera Vulnerability Exploits On The Rise

Figure 8 provides a visual representation of the trends in exploitation activity throughout the first quarter. The dashed line shows the moving average of this activity, while the solid line shows the actual weekly figures, highlighting any unusual spikes in the data.

When comparing Q4 2023 to Q1 2024, Nuspire observed a large increase, spurred mainly by massive increases in attempts against vulnerabilities like Hikvision's camera systems, Apache's Log4j and Wind River's VxWorks. This activity drove Q1's total levels of activity up **52.61%** when compared to Q4.

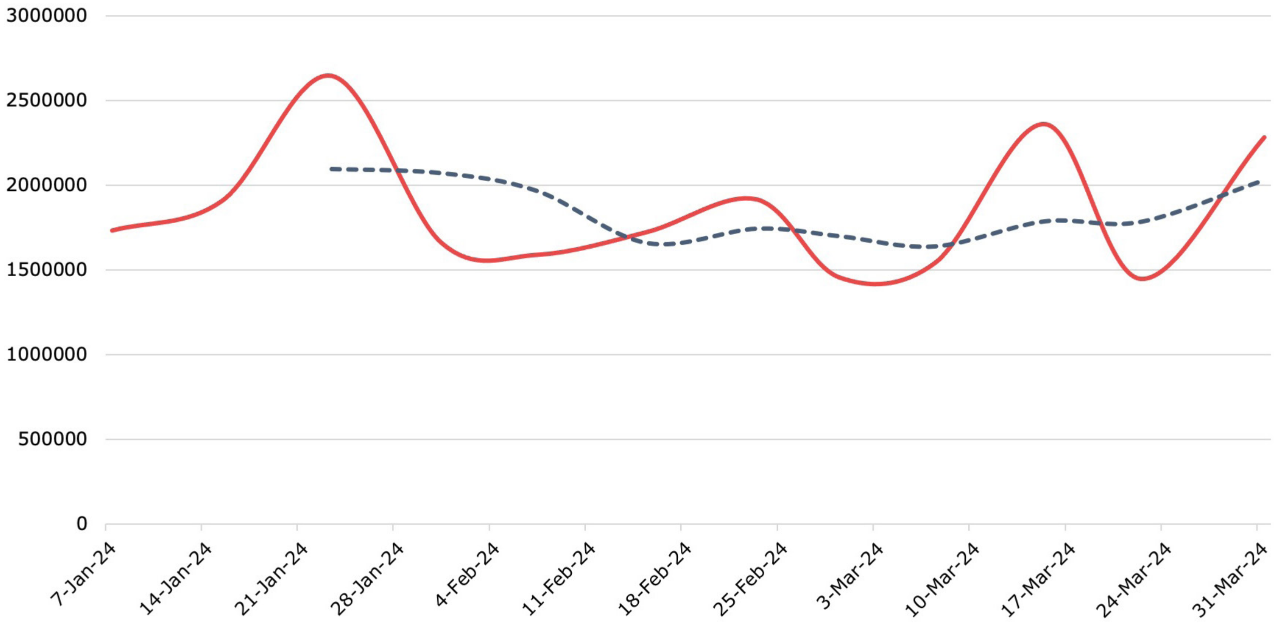


FIGURE 8. Q1 EXPLOIT ACTIVITY | NUSPIRE, Q1 2024

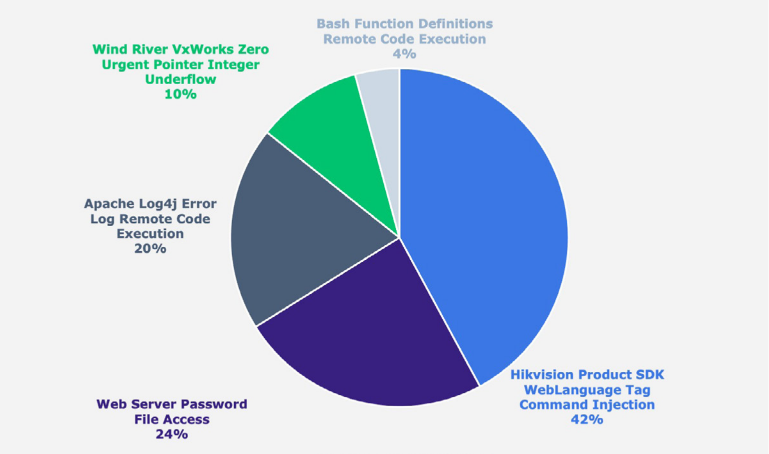


Figure 9 illustrates the most frequent exploit attempts observed in Q1. Q4's leading exploits, Web Server Password File Access and Apache Log4j, were surpassed in prevalence by attempts to exploit the Hikvision Product SDK WebLanguage Tag Command Injection vulnerability (CVE-2021-36260). This activity steadily built throughout the quarter.

FIGURE 9. Q1 TOP WITNESSED EXPLOITS | NUSPIRE, Q1 2024

Exploits

Hikvision Product SDK WebLanguage Tag Command Injection (CVE-2021-36260)

Nuspire observed a more than **twentyfold increase** in exploit attempts against this vulnerability compared to Q4's data, and momentum is steadily growing into Q2. Figure 10 shows the average exploitation activity against the Hikvision vulnerability in a dashed trend line. This Hikvision vulnerability is listed within CISA's **Known Exploited Vulnerability Catalog**, and has previously been deemed one of the top 20 exploited vulnerabilities.

The critically rated vulnerability (9.8/10 CVSS 3.1 scoring) affects Hikvision security cameras, allowing remote device hijacking without user interaction. Despite patches being available since 2021, threat actors still target this vulnerability due to the nature of IP camera systems, which are often plugged into a network and forgotten about. Operators of botnets, such as MooBot, have been observed leveraging this vulnerability to incorporate these devices into their networks.

Organizations using Hikvision IoT devices, like security cameras, should ensure that they are patched and segregated within your network to minimize chances of intrusion and any lateral movement a threat actor could take if they do gain access.

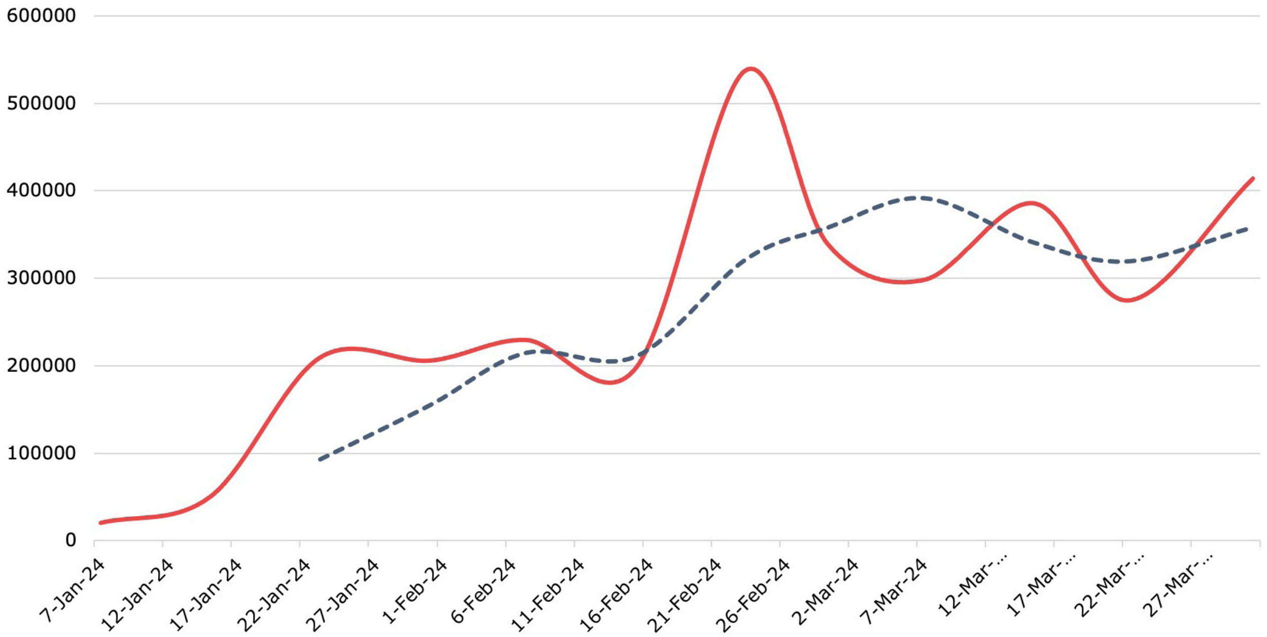


FIGURE 10. Q1 HIKVISION PRODUCT SDK WEBLANGUAGE TAG COMMAND INJECTION ATTEMPTS
NUSPIRE, Q1 2024

Microsoft Patch Tuesday Q1 2024 Summary

The widespread use of Microsoft products across organizations globally is well-known. This extensive adoption makes Microsoft's platforms a prime target for threat actors, who quickly exploit any announced or uncovered vulnerabilities as potent tools in their cyber arsenal. Here is the most recent compilation of critical and zero-day vulnerabilities announced by Microsoft for Q1.

DESCRIPTION	CVE	CVSS SCORING
Windows Hyper-V Remote Code Execution	CVE-2024-20700	7.5
Windows Kerberos Security Feature Bypass	CVE-2024-20674	8.8
Windows Kerberos Security Feature Bypass	CVE-2024-21351	7.6
Internet Shortcut Files Security Feature Bypass	CVE-2024-21412	8.1
Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege	CVE-2024-21400	9.0

FIGURE 11. Q1 MICROSOFT ZERO-DAYS | NUSPIRE, Q1 2024

Given the frequency at which vulnerabilities are exploited, it's vital for organizations to prioritize system updates. Microsoft issues regular updates known as Patch Tuesdays, which take place on the second Tuesday of each month at 1 p.m. EST. Administrators must stay informed about these updates and swiftly implement patches. Effective and prompt internal communication about upcoming updates is crucial, allowing organizations to proactively address vulnerabilities and thwart threat actors eager to exploit these openings.

Ways to Combat These Threats

In the world of cyber threats, timely action is essential for all involved parties.

Speedy system patching is crucial

Malicious actors continually scan for organizations that haven’t updated their systems and technologies with the latest patches. Therefore, it is vital for organizations to comprehend their technology stack thoroughly and promptly apply patches or mitigations as they become available. Particular focus should be given to vulnerabilities rated high or critical, especially those concerning remote access, as these are prime targets for attackers.

Install a firewall equipped with an intrusion prevention system (IPS)

Such a system can enhance network security by identifying and obstructing exploit attempts. Keeping the signature provided by your security vendor updated is essential to defend against the newest forms of attacks.

Stay informed through security news and vendor security bulletins

Protecting against new vulnerabilities is impossible without awareness of them. Organizations should consider enrolling in security bulletin services provided by most vendors, which are essential for receiving updates on patching and mitigation strategies. Regular monitoring of these updates is imperative.

Deactivate unnecessary services

Any unused service should be disabled to avoid introducing extra vulnerabilities. It’s also essential for organizations to understand which services are exposed to the internet and ensure their protection through VPN technology.

Rising Exploits and Dark Web Threats Require Vigilant Defense

The following are five simple actions security leaders can take to safeguard their organization and reduce the risk of breach.

1. Educate all users, often.

User awareness is one of the most powerful and cost-effective ways to defend your organization from a cyberattack. Educate your end users on how to identify suspicious attachments, social engineering and scams in circulation. Inform them on common theming, including any major events that could be created into a phishing lure. Establish procedures to verify sensitive business email requests (especially ones involving financial transactions) with a separate form of authentication in case an email account becomes compromised or is spoofed. Once an attacker has compromised an email account, they will often use the account as an additional layer of “authenticity” to attack within an organization.

2. Take a layered approach to security.

Buying single cybersecurity point products will not secure your business. A comprehensive ‘defense in depth’ approach with an integrated zero trust cybersecurity program protects businesses by ensuring that every single cybersecurity product has a backup. Integrating defense components counters any gaps in other defenses of security. Utilize vulnerability scanning to determine your weak spots and build your security around them. Enrich your logs with threat intelligence and perform threat modeling on your organization to determine how Advanced Persistent Threat groups are targeting your industry vertical.

3. Up your malware protection.

Advanced malware detection and protection technology (such as endpoint protection and response solutions) can track unknown files, block known malicious files and prevent the execution of malware on endpoints. Network security solutions, such as secure device management, can detect malicious files attempting to enter a network from the internet or laterally moving within a network. This advanced protection can provide threat responders additional tools like quarantining a specific device on the network and deep visibility into events happening on a device during investigations.

4. Segregate higher-risk devices from your internal network.

Devices that are internet-facing are high-value targets. Administrators should make sure to change the default passwords on these devices, as attackers are actively searching for devices that provide them easy access into a network. IoT devices should be inventoried, and a full understanding of your digital footprint is critical. Network segregation can help limit where an attacker can laterally move within an environment in the event of a breach.

5. Patch, patch and then patch some more.

Administrators should ensure that vendor patches are applied as soon as feasible within their environments. These critical patches can secure vulnerabilities from attackers. Administrators need to monitor security bulletins from their technology stack vendors to stay on top of newly discovered vulnerabilities attackers may exploit.

Cyber Resilience: Anticipating Tomorrow's Threats

With the ongoing advancement in cyber threats and techniques, attacks are progressively growing more complex and can cause extensive damage at a rapid pace. The silver lining is that cyberattacks can often be anticipated. Companies with internet connectivity or the possibility of internet connections must know they are potential targets. Consequently, these organizations should familiarize themselves with the most prevalent threats and evaluate their digital boundaries to determine the necessary steps for risk reduction.

Learn about the transformative impact of Managed Detection and Response (MDR) on your organization's ability to predict and respond to cyber incidents. - this would link to the MDR Product page.

Discover the benefits of incorporating dark web monitoring into your security posture to prevent identity theft and data breaches.

Fortify Your Defenses with Additional Resources from Nuspire

eBooks

Blogs

Videos

Reports

Webinars

Traversing the complexities of the contemporary digital landscape can pose challenges, but it need not be overwhelming. Reach out to us to secure assistance in safeguarding your organization against these recent threats.

About Nuspire

Nuspire, a leading managed security services provider (MSSP) with 25 years of experience, is revolutionizing the cybersecurity experience by taking an optimistic and people-first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @NuspireNetworks on X/Twitter.

nuspire.com
LinkedIn @Nuspire
X/Twitter @NuspireNetworks