blackpoint

EBOOK

The 5 Most Dominant Threat Actors of 2023

Table of Contents

Introduction

In the ever-evolving field of cybersecurity, recognizing the significant threat actors is essential. This year, we have seen five particularly influential cyber adversaries dominate: BlackCat, LockBit, QakBot, RedLine Stealer, and Akira. These groups have established themselves in the cyberthreat landscape with their unique tactics, techniques, and procedures (TTPs), along with their specific targets and business approaches.

This eBook examines the development, strategies, and innovative methods these actors use to attack and infiltrate systems. Additionally, it provides insights into effective countermeasures, helping organizations to strengthen their security measures against these advanced cyberthreats.

“In compiling our list, we found it interesting to note that two of the five threat actors—BlackCat and LockBit—were also mentioned throughout a blog we wrote back in February of 2023, titled, “2023 Cyberthreats to Watch Out For.” In addition to BlackCat research from the spring of 2022 and a technical analysis of a possible QakBot attack in early 2023, this foresight highlights what we’ve set out to do—proactively identify and prepare for emerging cyberthreats, said David Rushmer, Director of Threat Research. “Together, we can stay ahead of cyber adversaries and equip the businesses we protect with the necessary insight and tools to combat evolving threats.”

Tactics, Techniques, and Procedures (TTPs) Observed

Access Token Manipulation
Tampering with access tokens to gain higher privileges, allowing more extensive control over the system.

Command and Control (C2) Activities
Maintaining communication with infected hosts, often for issuing further instructions or data exfiltration. These activities frequently employ sophisticated techniques, including the use of non-standard ports & protocols, to effectively control infected devices.

Credential Access
Malware specializing in stealing various types of credentials from various locations.

Credential Theft and Web Injection
Stealing credentials, often through injecting malicious code into web processes, enabling the theft of sensitive data like banking details.

Data Encryption for Impact
Encrypting data on victims' infected systems, making it inaccessible & causing operational disruptions.

Data Collection and Exfiltration
Engaging in extensive data collection from compromised devices & exfiltrating this information over its C2 channel.

Defacement
Altering the appearance of webpages or system interfaces, which can be used for intimidation or to communicate demands.

Delivering Other Malware
Serving as a delivery mechanism for other types of malware, further compromising infected systems.

Disk Wipe
Deleting or corrupting data on the hard drive, which can lead to irreversible data loss & system damage.

Double Extortion for Ransomware
Encrypting data and then threatening to leak or delete it.

Exploitation of Zero-Day Vulnerabilities
Exploiting newly discovered vulnerabilities that haven't been patched yet.

Inhibit System Recovery
Disabling or corrupting system recovery options, making it harder to restore the system to a pre-infection state, prolonging downtime.

Initial Access via RDP Exploitation
Gaining initial access to networks by exploiting vulnerabilities in Remote Desktop Protocol (RDP).

Lateral Movement
Moving through a network and compromising additional systems. This is often achieved using compromised credentials, allowing the attackers to broaden their access within the network to deliver payloads or exfiltrate more data.

Network Enumeration
Using malware to scan a network to identify connected systems, devices, & their vulnerabilities, which can be exploited to extend its reach.

Phishing
Tricking users into revealing sensitive info or downloading malware, typically through phishing emails. It is sometimes combined with other social engineering techniques, serving as a primary method for gaining initial access to systems.

Process Injection
Injecting malicious code into legitimate processes to evade detection & execute its payload stealthily.

Targeting Specific Operating Systems
Targeting a specific operating system such as Linux, Microsoft Windows, or macOS, indicating a specific focus on enterprise-level infrastructure.

Use of Legitimate Tools for Reconnaissance and Credential Dumping
Using legitimate administrative tools on the victim's system to gather information about the system or network and to extract sensitive login information.

User Execution
Relying on users executing the malware, often through opening infected email attachments or clicking malicious links.

BlackCat

ALIASES:
ALPHV, AlphaV, Noberus

EMERGENCE:
Mid-November 2021

BlackCat, a Ransomware-as-a-Service operation, is a possible rebranding of the group DarkSide. They were the first ransomware group to create a public data leaks site, and target large enterprises, such as MGM Resorts in September 2023. BlackCat is written in Rust, enabling them to target Windows and Linux. Most recently, they filed an SEC complaint against a victim for not disclosing a cyberattack.

BlackCat

EVOLUTION:

BlackCat represents a new wave of ransomware threats, evolving from previous ransomware groups like DarkSide and BlackMatter.

BUSINESS MODEL:

- Operates under a Ransomware-as-a-Service (RaaS) model, where developers offer malware to affiliates in exchange for a percentage of the ransom payments.
- Known for its sophisticated double and sometimes triple extortion tactics.
  - Recently escalated to filing an SEC complaint against a victim for not disclosing a cyberattack.

INNOVATIVE TECHNIQUES:

Notable for being the first ransomware to create a public data leaks site on the open internet, and for employing typo-squatted replicas of victim websites to post stolen data, enhancing the pressure on victims.

TARGET PROFILE:

- Broad range of global targets including universities, government agencies, and companies in the energy, technology, manufacturing, and transportation sectors.
- Recent highly impacted targets include MGM Resorts International and Caesars Entertainment.

ASSOCIATED GROUPS:

Linked to discontinued RaaS groups like DarkSide and BlackMatter. Speculations suggest it might be a rebranding of DarkSide or a successor to REvil.

Top 5 TTPs and How to Stay Ahead of Them:

Data Encryption for Impact

Mitigation:

- Maintain regular, offline backups of critical data.
- Ensure backups are stored in a separate environment and are tested regularly for integrity and quick restoration.

Disk Wipe

Mitigation:

- Implement file integrity monitoring systems to detect and alert on mass deletion or modification of data.
- Regularly back up data and system configurations.

Defacement

Mitigation:

- Use monitoring tools to detect changes in system configurations or files.
- Regularly review and update website security measures to prevent unauthorized access.

Inhibit System Recovery

Mitigation:

- Protect and regularly test backup and recovery processes.
- Ensure mechanisms like shadow copy are not tampered with and are accessible in emergencies.

Access Token Manipulation

Mitigation:

- Employ security tools that monitor and audit token manipulations and unusual process behaviors.
- Regularly update and enforce strict access control policies.

Related Resources:

Malware on Trial

Read the Blog

FIN8's Latest Remix: Sardonic with Noberus

Read the Blog

Viva Las Vulnerabilities: MGM Hit by ALPHV Ransomware

Read the Blog

LockBit

ALIASES:
ABCD Ransomware

EMERGENCE:
September 2019

LockBit is well known for its continuous evolution through versions 2.0 and 3.0. They operate as a Ransomware-as-a-Service and have been known to recruit insiders from the companies they target. They tend to target healthcare facilities and schools, in particular, those with devices running the Linux operating system (OS).

LockBit

EVOLUTION:

LockBit has evolved significantly since its inception, with notable advancements seen in LockBit 2.0 and 3.0 versions. LockBit 2.0 surfaced in June of 2021 and 3.0 in March of 2022. These evolutions include improved encryption methods, targeting strategies, and the introduction of innovative tools like "StealBit" for data exfiltration.

BUSINESS MODEL:

Operates as a RaaS group, using double extortion tactics involving encryption and data leak threats. They also offer the ransomware to affiliates and share profits from ransom payments.

INNOVATIVE TECHNIQUES:

- Developed “StealBit” for efficient data exfiltration.
- Targets Linux hosts, focusing on ESXi servers, showcasing its adaptability and technical sophistication.

TARGET PROFILE:

Predominantly targets the healthcare and education sectors, with significant attacks in the United States, India, and Brazil.

ASSOCIATED GROUPS:

Collaborates with various criminal groups and network access brokers, even recruiting insiders from targeted companies.

TOP 5 TTPS AND HOW TO STAY AHEAD OF THEM:

Initial Access via RDP Exploitation

Mitigation:

- Enhance RDP configurations to ensure they are secure.
- Implement multifactor authentication to add an extra layer of security.
- Maintain vigilant monitoring of RDP access logs for any signs of unauthorized attempts.

Phishing

Mitigation:

- Conduct comprehensive phishing awareness training for employees.
- Deploy advanced email filtering systems to catch phishing attempts.
- Utilize phishing detection technologies to identify and block malicious content.

Data Encryption for Impact

Mitigation:

- Regularly maintain offline backups and ensure they aren’t connected to the primary network to avoid simultaneous encryption.
- Frequently test these backups for integrity and quick restoration capabilities.

Use of Legitimate Tools for Reconnaissance and Credential Dumping

Mitigation:

- Implement behavior-based anomaly detection systems that can identify unusual use of these tools.
- Conduct regular audits to spot any unauthorized or suspicious activities involving these tools.

Lateral Movement

Mitigation:

- Strengthen credential security with robust password policies and multifactor authentication.
- Regularly monitor network traffic and logs for unusual access patterns that might indicate lateral movement.
- Implement strict access control measures to limit the reach of compromised credentials.

Related Resources:

Cisco ASA SSL VPN Appliances Under Fire

Read the Blog

APG Threat Digest on Nov. 20, 2023

Read the Blog

QakBot

ALIASES:
Qbot, Quackbot, Pinkslipbot, TA570

EMERGENCE:
2008. They are one of the long-standing threats in the cyber landscape.

QakBot is a versatile botnet that offers a suite of tools, often setting the stage for Conti, Egregor, and others' ransomware deployments. Despite government interference, QakBot continues to return with new, innovative tactics.

QakBot

EVOLUTION:

Initially a banking trojan, QakBot has transformed into a versatile botnet, constantly updating to include more sophisticated functionalities. In 2023, their infrastructure was taken down in a government operation. In that time, DarkGate and PikaBot may have been spinoffs of QakBot. In December 2023, though, QakBot returned with novel tactics.

BUSINESS MODEL:

QakBot is not limited to a single type of cybercrime. It offers a suite of tools for reconnaissance, lateral movement, data gathering, and exfiltration, and serves as a vector for delivering various malicious payloads.

TARGET PROFILE:

Focuses on global infrastructures with an emphasis on sectors like finance, emergency services, commercial facilities, and election infrastructure subsectors.
Most recently, they targeted the hospitality industry.

ASSOCIATED GROUPS:

Often sets the stage for the deployment of human-operated ransomware like Conti, ProLock, and Egregor, among others.

TOP 5 TTPS AND HOW TO STAY AHEAD OF THEM:

Credential Theft and Web Injection

Mitigation:

- Implement advanced web filtering and threat detection solutions.
- Regularly update antivirus and anti-malware programs to detect and block such injections.

Network Enumeration

Mitigation:

- Regularly monitor your network and perform vulnerability assessments.
- Employ network segmentation to limit the spread of malware.

Lateral Movement

Mitigation:

- Use network monitoring tools to detect unusual traffic patterns indicative of lateral movements.
- Employ strict access controls and segment networks to minimize access.

Process Injection

Mitigation:

- Implement behavior-based detection systems that can identify unusual activities in standard processes.
- Regularly update security software to detect sophisticated process injections.

Delivering Other Malware

Mitigation:

- Continuously monitor network and system activities for signs of secondary payload deployment.
- Ensure that security systems are capable of detecting and isolating diverse malware types.

Related Resources:

With .one Foot in the Door

Read the Blog

A Glimpse at Ransomware Roundup

Read the Blog

Blackpoint Detains QakBot Information-Stealing Malware

Read the Case Study

RedLine Stealer

ALIASES:
No known aliases

EMERGENCE:
March 2020

RedLine Stealer is known for its extensive information-gathering and data exfiltration capabilities. It operates as a Malware-as-a-Service and is used by a wide range of cybercriminals. RedLine attacks often target industries such as healthcare and manufacturing.

RedLine Stealer

EVOLUTION:

RedLine Stealer has been continuously updated, showing an ability to adapt and enhance its data exfiltration capabilities. It's known for its extensive information-gathering features, including the ability to load remote payloads.

BUSINESS MODEL:

Operates as Malware-as-a-Service (MaaS) offered on underground forums with different pricing tiers, including lite, pro, and subscription options, paid for with cryptocurrencies.

INNOVATIVE TECHNIQUES:

Collects an array of data from users' browsers, including sensitive login information, auto-fill form fields, and browser history. Utilizes SOAP API for C2 communication and leverages Telegram API for real-time infection notifications.

TARGET PROFILE:

Impacts a wide range of sectors, notably healthcare and manufacturing.

ASSOCIATED GROUPS:

Distributed to a range of cybercriminals on the dark web, indicating a broad base of users rather than specific associated groups.

TOP 5 TTPS AND HOW TO STAY AHEAD OF THEM:

Phishing

Mitigation:

- Implement comprehensive phishing awareness training.
- Advanced email filtering and anti-phishing technologies.

Credential Access

Mitigation:

- Use robust password management solutions.
- Enable multifactor authentication.
- Regularly update passwords to secure accounts.

User Execution

Mitigation:

- Restrict the execution of unknown or untrusted applications and files.
- Implement user training programs to educate on safe computing practices.

Data Collection and Exfiltration

Mitigation:

- Employ endpoint detection and response (EDR) tools to monitor for data exfiltration activities.
- Regularly scan systems for unauthorized data access and transmission.

Command and Control (C2) Activities

Mitigation:

- Implement network monitoring solutions to detect unusual network traffic and C2 communications.
- Update and enforce network security policies and firewall rules.

Related Resource:

APG Threat Digest on Nov. 13, 2023

Read the Blog

Akira

ALIASES:
Akira Ransomware

EMERGENCE:
March 2023

Akira is known for its distinctive, retro-style Tor leak site, where they offer victims the choice between paying for decryption or data deletion. They utilize leaked source code of Conti ransomware, suggesting collaboration of some sort. Akira typically targets Linux machines and VMware ESXi virtual machines.

Akira

EVOLUTION:

It is different from the Akira ransomware active in 2017, but uses the same ".akira" extension for encrypted files. Akira utilized the leaked source code of Conti ransomware, demonstrating an evolution in its technical capabilities.

BUSINESS MODEL:

Akira operates by performing double extortion, offering victims the choice between paying for decryption or data deletion. Ransom demands typically range from $200,000 to over $4 million.

INNOVATIVE TECHNIQUES:

Features a distinctive retro-styled Tor leak site, setting it apart in presentation and style. Exploited a zero-day vulnerability (CVE-2023-20269) in Cisco products to establish unauthorized VPN sessions, indicating a high level of technical sophistication.

TARGET PROFILE:

Expanded targets to include Linux machines and VMware ESXi virtual machines. Initially, it heavily impacted the healthcare industry, as indicated by alerts from the U.S. Department of Health and Human Services. They are present predominantly in the US and Canada.

ASSOCIATED GROUPS:

Shared code similarities with Conti ransomware actors, suggesting collaboration or shared knowledge among these cybercriminal groups.

TOP 5 TTPS AND HOW TO STAY AHEAD OF THEM:

Exploitation of Zero-Day Vulnerabilities

Mitigation:

- Keep all software and systems up to date with the latest patches, especially those addressing known vulnerabilities.
- Regularly conduct vulnerability assessments.

Double Extortion for Ransomware

Mitigation:

- Maintain regular, secure, and isolated backups of critical data.
- Ensure backup integrity and quick restoration capabilities.

Phishing

Mitigation:

- Conduct regular cybersecurity awareness training focusing on recognizing and reporting phishing attempts.

Targeting Specific Operating Systems

Mitigation:

- Implement additional security measures and monitoring tools for Linux environments and virtual machine infrastructure.
- Regularly update and patch these systems.

Command and Control (C2) Activities

Mitigation:

- Employ advanced network monitoring to detect and block unauthorized C2 communications.
- Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) for additional network protection.

Related Resource:

Cisco ASA SSL VPN Appliances Under Fire

Read the Blog

In Conclusion

Understanding the key players and their methods in the 2023 cyberthreat landscape is essential for effective cybersecurity. The distinct approaches of BlackCat, LockBit, QakBot, RedLine Stealer, and Akira highlight the need for targeted defensive strategies.

This analysis not only sheds light on their unique tactics but also suggests robust mitigation techniques. Staying updated and adaptable in cybersecurity practices is crucial for organizations aiming to safeguard themselves against these evolving threats. Keeping pace with these adversaries is critical to maintaining strong and resilient cyber defenses in today's challenging security environment.

Why Blackpoint Cyber?

Founded in 2014 by former National Security Agency (NSA) cyber operations experts, the Blackpoint team continues to bring nation-state-grade technology and tactics to our partners around the world. By fusing real security with real response, our elite SOC team is empowered by the proprietary technology we built from the ground up.

Together, we detect breaches faster than any other solution on the market. With insight into network visualization, tradecraft detection, endpoint security, suspicious events, and remote privileged activity, Blackpoint detects lateral movement in its earliest stages and stops the spread.

By the time you hear from us, the threat has been triaged and removed, often before the malicious actor even saw us coming. Lastly, we optimize our architecture and data to its fullest extent, ensuring robust services and valuable intel for our partners. That way, critical facets of security—on-prem & cloud response, endpoint protection, application control, logging, and cyber insurance—can work in tandem to support an integrated cyber strategy. Sleep easy knowing we detect and detain threats on your behalf around the clock.

Our mission? To provide unified, 24/7 detection and response services to organizations of all sizes around the world.

SIGN UP FOR A DEMO TODAY!

CONTACT US

info@blackpointcyber.com

blackpointcyber.com