CYBER THREAT INTELLIGENCE REPORT

FIRST HALF 2023

CRITICALSTART®

Table of Contents

Cyber Threat Intelligence Research

As technology advances, so does the digital threat landscape.

While cyberattacks continue to become increasingly sophisticated and widespread, the need for effective cyber threat intelligence (**CTI**) is even more essential.

Historically, the first quarter has proven to be busy for the Critical Start security operations center (**SOC**) team, and this year was no exception. Throughout this report, we will explore the top threats from the First Half (**H1**) of 2023 and summarize emerging trends that have implications across various industries.

By using the knowledge in this research report, organizations can make informed decisions, prioritize resources effectively, and better protect themselves from prevalent and evolving threats.

Cyber Threat Intelligence Trends

- From the beginning of January through the end of April 2023, the Critical Start SOC saw overall increases in the number of investigated alerts, alerts escalated to customers, and alerts that were of high or critical priority. Moreover, in the first quarter of 2023, the SOC observed a significant 38.88% increase in the number of high or critical priority alerts over the previous quarter.

- Two-step phishing attacks are on the rise, with attackers using convincing emails that resemble legitimate vendor communications, often related to electronic signatures, orders, invoices, or tracking information.
- State-sponsored cyber espionage is becoming increasingly common, with threat actors operating out of Russia, potentially India, and the Asia-Pacific (**APAC**) region.
- The new Beep malware is top of mind for organizations and individuals. This pervasive threat is delivered via email attachments, Discord, and OneDrive URLs.

[1] *MarketsAndMarkets. Managed Detection and Response (MDR) Market Report. (MarketsAndMarkets, 2022)*

Top 10 Threats of H1 2023

In this report, the Critical Start CTI team has detailed top threats from H1 2023, along with insights that can enable organizations to strengthen their security posture and proactively mitigate potential risk.

Each section includes an executive summary of CTI's Top 10 Threats, with a link to the full research write-up for a complete technical deep dive.

LockBit Announces New Variant

Threat: LockBit Green

Type of Threat: Ransomware-as-a-Service (**RaaS**)

Targeted Industries: Small and medium-sized businesses

LockBit, a Russian-based ransomware group, has recently announced the release of a new variant called LockBit Green. This variant shares similarities with the Conti ransomware, as it incorporates a large portion of Conti's leaked source code. LockBit ransomware group operates under a RaaS model leveraging double, and sometimes triple, extortion techniques. It's estimated LockBit had **nearly 1100 victims in 2022 alone.**

LockBit has a history of developing new variants, including LockBit Red (**LockBit 2.0**) released in June 2021 and LockBit Black (**LockBit 3.0**) released in May 2022, which borrowed heavily from the BlackMatter ransomware code. LockBit Green, announced in February 2023, primarily uses code from the leaked Conti source code. Additionally, LockBit has released a Linux/ESXi alternative that uses Advanced Encryption Standard (**AES**) and Elliptic curve cryptography (**ECC**) encryption, as well as an information stealer called StealBit that supports affiliates by grabbing and uploading victim data to the LockBit victim-shaming site.

Read More

Emotet Returns After Months of Silence

Threat: Emotet

Type of Threat: Malware

Targeted Industries: Healthcare, government, banking, education, small businesses

After a brief hiatus, Emotet threat actors resumed their operations in early March 2023. Emotet, originally a banking trojan, has transformed into a versatile piece of malware that relies on massive spam email campaigns. Using a technique called email hijacking, the attackers insert themselves into existing business conversations or initiate new email conversations to make the malicious emails appear trustworthy. They often employ urgency-inducing topics, like service invoices, to increase the chances of victims opening the emails.

The malicious emails typically contain a .ZIP file attachment with an infected Word document that prompts the user to enable macros. Once enabled, Emotet downloads its Digital Link Library (**DLL**) from an external site and loads it into memory. It then awaits instructions from a remote command and control server, often leading to the download of additional payloads, including ransomware.

As Microsoft moves towards disabling macros by default, Emotet operators are expected to adopt new delivery formats for the malware.

Read More

Top 10 Threats of H1 2023

Microsoft Outlook Zero-Day Exploited in the Wild

Threat: Microsoft Outlook Zero-Day Vulnerability

Type of Threat: Zero-day vulnerability leading to elevation-of-privilege (**EoP**) and remote code execution

Targeted Industries: Government, transportation, energy, military

Microsoft recently disclosed a zero-day vulnerability in Outlook, identified as CVE-2023-23397. This elevation-of-privilege flaw allows threat actors to execute remote code and steal NTLM credentials of Outlook users. The impact of this vulnerability extends to all supported versions of Microsoft Outlook for Windows. However, web-based Microsoft 365 is not vulnerable as it does not support Windows New Technology LAN Manager (**NTLM**) authentication.

Although the hacking group remains undisclosed, Microsoft has linked it to Russian military intelligence. To mitigate the risk, Microsoft recommends organizations block outbound Server Message Block (**SMB**) port 445 traffic to prevent NTLM authentication messages from being sent to remote file shares. Additionally, adding users to the Protected Users security group restricts the use of NTLM as an authentication method.

Read More

Two-Step Phishing Attacks

Threat: Two-Step Phishing Attacks

Type of Threat: Phishing

Targeted Industries: All industries

Two-step phishing attacks involve threat actors using compromised vendors to target potential victims by creating convincing emails that resemble legitimate vendor communications, often related to DocuSign, orders, invoices, or tracking information. By utilizing the same applications as the vendor, the attackers reduce detection risks. Victims are directed to fake login pages where they may unwittingly input their credentials.

These attacks exploit the credibility of compromised vendors and are successful in obtaining sensitive information. It is crucial for individuals to verify URLs before entering credentials and consider implementing multi-factor authentication (**MFA**). Organizations should prioritize strong cybersecurity measures, employee training, and regular security protocol updates to mitigate these threats.

Read More

Top 10 Threats of H1 2023

Black Lotus

Threat: BlackLotus

Type of Threat: Malware

Targeted Industries: Wide range of industries

BlackLotus is a stealthy Unified Extensible Firmware Interface (**UEFI**) bootkit, a type of malware that can circumvent Secure Boot defenses. It is the first known malware capable of bypassing Secure Boot on fully up-to-date Windows 11 systems with UEFI Secure Boot enabled.

Mitigating BlackLotus is challenging, but organizations and individuals can take several steps to reduce the risk of a successful attack. Keeping systems up to date, using security software, enabling Secure Boot, implementing multi-factor authentication, network segmentation, conducting regular security assessments, and **enforcing strong password policies** can help mitigate the threat. However, it's important to note that these measures cannot completely eliminate the risk, emphasizing the need for ongoing vigilance and monitoring of the threat landscape.

Read More

Clasiopa

Threat: Clasiopa, a sophisticated threat actor

Type of Threat: Custom-developed malware and hacking tools

Targeted Industries: Materials research industry

Clasiopa is a sophisticated threat actor that utilizes a distinct toolset that includes custom-developed malware and hacking tools. Clasiopa's primary malware is Backdoor.Atharvan, a remote access Trojan (**RAT**) designed to evade detection. They also use modified versions of Lilith RAT for remote control and Thumbsender for gathering and exfiltrating file names. A custom proxy tool helps them maintain persistence and communicate with command-and-control servers undetected.

Clasiopa's origins and motivations remain unknown. While **some evidence suggests a possible connection to India**, it could be intentional misdirection. Further research is needed for conclusive attribution. Organizations in the materials research industry should implement robust security measures, including software updates, employee education, and advanced threat detection.

Read More

Beep Malware

Threat: Beep Malware

Type of Threat: Botnet Implant Malware

Targeted Industries: Windows Endpoint OS

Beep is a newly discovered botnet implant malware that employs exhaustive anti-analysis and detection-evasion techniques. It enables attackers to remotely deploy additional malware payloads onto compromised systems. The malware consists of a dropper, an injector, and an implant payload, with the capability to gather host information and communicate with a command and control (**C2**) server for further instructions. Beep exhibits advanced evasion tactics and is still in the early stages of development, with potential for future functionality enhancements.

Read More

Top 10 Threats of H1 2023

Dark Pink

Threat: Dark Pink (Saaiwc Group)

Type of Threat: Advanced Persistent Threat (**APT**) group using tailored spear-phishing attacks

Targeted Industries: Government agencies, military organizations, religious groups, non-profit organizations

Dark Pink is an emerging APT group that has been active since mid-2021, with their first successful attack observed in June 2022. The group **operates in the APAC region** and employs sophisticated techniques, including DLL side-loading and Event Triggered Execution, to launch custom malware and maintain persistence. Their attacks begin with tailored spear-phishing emails disguised as job applications, containing personalized Information Security Officer (**ISO**) images that include signed executables, decoy documents, and malicious DLL files. Dark Pink infects both the victim's device and any removable drives present, using the Telegram API for communication and data exfiltration.

Dark Pink's primary objectives are corporate espionage, document theft, audio capture using infected device microphones, and data exfiltration from messengers.

Dark Pink's sophisticated attacks pose a significant threat, requiring organizations to implement robust security measures. Vigilance, employee training, and strengthening email security solutions are crucial to detecting and preventing Dark Pink's spear-phishing campaigns. Organizations in the APAC region should be proactive in defending against this APT group's activities.

Read More

DarkCloud

Threat: DarkCloud Information Stealer Malware

Type of Threat: Information stealer malware, phishing emails

Targeted Industries: Windows endpoint operating systems

DarkCloud is an information stealer malware delivered through phishing emails with malicious attachments. It can extract usernames, passwords, credit card data, and sensitive information from various applications and browsers.

Organizations should prioritize employee training, awareness, and strong cybersecurity measures to protect against this threat.

Read More

Top 10 Threats of H1 2023

Malware Targeting Linux Operating Systems

Threat: Malware targeting Linux Operating Systems

Type of Threat: Advanced malware, botnets, ransomware, cryptojacking

Targeted Industries: Organizations using Linux systems, including cloud services, government entities, managed services providers, and organizations using Kubernetes clusters and containerized environments

Linux, known for its security advantages, was previously considered less vulnerable compared to other operating systems. However, with Linux being widely used in critical areas of businesses and cloud services, threat actors have shifted their focus and developed sophisticated malware to target Linux. Several active ransomware groups, such as **LockBit, AvosLocker, and Luna**, are now targeting Linux systems using vulnerabilities and penetration testing tools like Cobalt Strike and Vermilion Strike.

Linux users should be aware of the increased targeting and adopt security best practices to minimize access for threat actors. User awareness around social engineering and cyber security vigilance should be emphasized, and a Linux-based security approach should be developed to protect against various threats.

Read More

Protecting your Organization

To help protect against these emerging and evolving threats, organizations should consider taking these actions:

Employee Training and Awareness Focus: Investing in employee training and awareness programs is a fundamental step in mitigating cyber risks. By educating employees on the latest threat landscape, signs of phishing emails, and promoting best practices for cybersecurity, organizations can create a human firewall that acts as an additional layer of protection.

Regular Security Protocol Updates: Keeping security protocols up to date is essential to stay resilient against evolving threats. Critical Start recommends regular updates to security protocols based on industry best practices and emerging threat intelligence. This proactive approach ensures that your organization remains well-prepared to detect, respond to, and mitigate potential vulnerabilities.

Collaboration with Trusted Partners: Working with trusted partners like Critical Start provides access to specialized expertise and cutting-edge security solutions. Critical Start's Managed Detection and Response (**MDR**) services, powered by Zero-Trust Analytics Platform® (**ZTAP**®), deliver 24x7x365 monitoring, investigation, and response capabilities. The MDR services include triage of security events, tailored response actions, and ongoing security guidance to strengthen your infrastructure.

Critical Start's SOC guarantees one-hour SLAs for Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) on every alert. That's not a goal – that's a promise. Let us sort through the noise and do the heavy lifting. Connect with an expert to talk about your cybersecurity challenges today.

To stay ahead of emerging threats, the Critical Start Cyber Threat Intelligence (**CTI**) team leverages a variety of intelligence sources, including open-source intelligence, social media monitoring, and dark web monitoring.

As a part of the Critical Start Cyber Research Unit (**CRU**), CTI will continue to monitor emerging threat developments and work closely with the Security Engineering and SOC teams to implement any relevant detections. For future updates on emerging threats, follow our Critical Start Intelligence Hub.

For more information, contact us at:
criticalstart.com