CYBER THREAT INTELLIGENCE REPORT

SECOND 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.

In this report, we will delve into prominent threats and outline emerging trends with implications spanning multiple industries. Leveraging the insights contained in this research report, organizations can make well-informed decisions, allocate resources strategically, and enhance their defenses against both current and evolving threats.

Cyber Threat Intelligence Trends

Throughout the duration spanning from May 2023 to the conclusion of August 2023, Critical Start's team of dedicated analysts diligently harnessed both internal and external resources to meticulously identify and scrutinize security events of paramount significance. This multifaceted effort was driven by the overarching goal of not only recognizing high-priority security events but also comprehending the evolving landscape of cyber trends, thus ensuring an enhanced preparedness to address emerging threats and vulnerabilities.

- The Critical Start Cyber Operations Risk & Response™ platform ingested 583,698,951 security events
- Critical Start Risk and Security Operations Center (**RSOC**):
  - Investigated 48,906 alerts
  - Escalated 13,910 alerts to clients
    - 1,142 of these alerts were High or Critical
  - Isolated 1,805 consoles

Trending Cyber Events

- Microsoft Teams allows external accounts to send potentially harmful files directly to an organization's staff, increasing the risk of successful attacks by bypassing security measures and anti-phishing training.
- Quick Response (**QR**) codes are being utilized in a new phishing campaign as a means to gather Microsoft credentials from unsuspecting victims. This campaign has targeted various industries, with the energy sector being the most heavily impacted.
- The practice of multiple threat actors employing identical detailed tactics, techniques, and procedures (**TTPs**) can present a notable threat, as such coordination often leads to more sophisticated and effective attacks than individual actions would permit. https://www.criticalstart.com/understanding-the-resurgence-of-kerberoasting-attacks-in-todays-threat-landscape/

Top 10 Threats of H2 2023

In this report, the Critical Start CTI team has detailed top threats from H2 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 report to gain a complete technical deep dive.

Microsoft Teams Vulnerabilities

Threat: Microsoft Teams Vulnerability

Type of Threat: External accounts delivering malicious files

Targeted Industries: All Industries

Security researchers based in the UK discovered a bug in the latest version of Microsoft Teams that allows external accounts to deliver potentially malicious files to an organization's employees. Delivering files directly via Teams bypasses nearly all existing security measures and anti-phishing training advice, increasing the likelihood of a successful attack. The flaw exists in the default configuration of Microsoft Teams, which allows communication with Teams accounts outside the company, known as external tenants. Even though blocks are in place to prevent file delivery from external accounts, simply changing the internal and external recipient ID in the POST request message can fool the system into treating the external actor as an internal authorized user. When exploiting this flaw, the file is hosted on a SharePoint domain and appears as a file in the target's Teams inbox, not as a link. Hiding behind the SharePoint domain also lends legitimacy to the file and increases the likelihood that the target will open the file.

Microsoft confirmed the existence of the flaw; however, they stated it did not meet the threshold for immediate servicing. It's recommended that any organization utilizing Teams review their business requirement for communication with external tenants. If regular communication with external tenants is not required, this feature should be disabled from Microsoft Teams Admin Center > External Access. After review, if it's determined that communication with external tenants is needed, organizations should define only specific domains in an allow-list to lower the risk of exploitation.

Read More for Risks & Mitigations

Top 10 Threats of H2 2023

MOVEit

Threat: Ransomware

Type of Threat: Software supply chain attacks

Targeted Industries: All Industries

The recent surge in ransomware attacks targeting software supply chains, exemplified by the exploits on MOVEit, GoAnywhere, and 3CX Desktop Client, underscores the intensifying threat landscape and the imperative for robust security measures. The successful exploitation of vulnerabilities in MOVEit, GoAnywhere, and 3CX Desktop Client underscores the gravity of supply-chain attacks, revealing several pivotal implications:

- Heightened Exposure: Software solutions within the managed file transfer (**MFT**) category, like MOVEit, frequently house sensitive data, encompassing regulated information, intellectual property, and critical organizational data. The exposure of such data carries substantial risks, including legal repercussions and damage to reputation.
- Evolving Tactics: Clop's adoption of novel tactics, including publicly announcing attacks and demanding ransoms, intensifies pressure on organizations. This approach seeks to maximize the impact on susceptible software versions and further solidify Clop's standing within the cybercriminal realm.

This strategic intelligence report delves into the observed trends within these attacks and their broader ramifications for organizations employing similar software solutions. It offers a comprehensive risk assessment and strategic recommendations for mitigating these threats, with particular emphasis on managing vendor relationships.

Read More for Risks & Mitigations

Credential Harvesting

Threat: Credential Harvesting

Type of Threat: 'Pretexting' where the threat actor invents a scenario that tricks the user into giving up their credentials

Targeted Industries: Energy, Manufacturing, Insurance, Software & IT, Finance

A study conducted in 2023 revealed that a significant 41% of security breaches have involved the illicit use of stolen credentials. Cyber adversaries consider human error the foremost cybersecurity threat, and they often find it more convenient to target individuals within organizations for the purpose of harvesting login information rather than attempting to breach the technical elements of an IT system. In 2022, an estimated 54% of all social engineering attacks employed a technique known as 'pretexting,' where threat actors fabricate scenarios to deceive users into disclosing their credentials or performing actions that benefit the attacker. This method is frequently deployed through phishing campaigns. Additionally, former employee credentials are frequently exploited because organizations neglect to deactivate these accounts, providing threat actors with an uncomplicated route to bypass security measures and operate undetected. These tactics have elevated credential harvesting as one of the primary attack vectors employed to infiltrate organizations.

The repercussions of falling victim to credential harvesting can be severe. Attackers can leverage compromised accounts for financial gain, engage in identity theft by stealing personal information, or use the stolen credentials to launch additional attacks, establishing a foothold in the target's systems. For businesses, the aftermath may entail data breaches, reputational damage, financial losses, and potential legal liabilities.

Credential harvesting techniques represent a persistent threat in today's digital landscape. It is imperative for both individuals and organizations to comprehend these methodologies and recognize their potential impact. By staying well-informed, adhering to sound security practices, and investing in robust cybersecurity measures, organizations can fortify their defenses against cybercriminals who exploit the vulnerabilities of credential harvesting.

Read More for Risks & Mitigations

Top 10 Threats of H2 2023

Attack Vectors within the Education Sector

Threat: Cyber Threat Actors

Type of Threat: Common vulnerabilities and exposures, phishing campaigns, cryptojacking, malware, and Ransomware-as-a-Service (**RaaS**)

Targeted Industries: Education

The education sector remains a prime target for cyber threat actors who continually adapt to evolving security measures and employ increasingly sophisticated targeting strategies. In the first half of 2023, the education industry witnessed a staggering 179% surge in cyberattack volume compared to the same period in 2022. Notably, these attacks have shifted towards K-12 institutions, which were previously less targeted compared to higher education establishments. Often, educational institutions lack robust IT infrastructure to safeguard vast repositories of sensitive data concerning students, faculty, and staff. Consequently, threat actors view the education sector as a lucrative opportunity with relatively low risks.

Cyber threat actors have developed a diverse array of attack vectors aimed at educational institutions, including vulnerability exploitation, phishing campaigns, cryptojacking, malware, and ransomware. Vulnerability exploitation accounted for 29% of attacks, while phishing campaigns constituted 30% of cyber incidents on K-12 schools in 2023. Cryptojacking incidents increased significantly, with a year-to-date rise of 320 instances, and the monthly targeting rate rose from 0.19% to 0.55%. Malware attacks against educational institutions rose slightly to 9.4% compared to 8.9% the previous year, with malware often being delivered in the form of malicious Microsoft OneNote files since February 2023. Additionally, ransomware attacks spiked by 84% in the first half of 2023 compared to the previous year.

The education sector relies on a wide range of networks to facilitate information sharing and remote access for various stakeholders, including students, instructors, parents, office staff, and administrators. However, this expansive network can leave educational institutions vulnerable if they do not allocate sufficient resources to cybersecurity. Schools bear the responsibility of safeguarding sensitive personal information, including birth records, social security numbers, addresses, and medical data. Unfortunately, limited government funding and a lack of cybersecurity awareness, especially among students, often hinder these institutions' ability to effectively protect their staff and students' information.

Read More for Risks & Mitigations

Top 10 Threats of H2 2023

Threat Actors Collaborating

Threat: Cyber Threat Actors

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

Targeted Industries: All Industries

Since the beginning of 2023, cyber threat research has revealed that several known ransomware groups are sharing TTPs at a granular level. It is likely this trend is due to new RaaS groups emerging and existing groups re-branding or shutting down operations. Due to the RaaS operating model, it is not uncommon for there to be crossover in groups and the TTPs they use. However, in the instances below, the similarities in TTPs suggest that the threat actors are using the same playbooks. These instances have been noted as cluster activity within the cyber security domain. These highly specific, unique behaviors suggest that the ransomware groups are much more reliant on affiliates than previously thought. This trend highlights the complex and ever-changing nature of the cybercrime economy.

Ransomware source code is extremely complex and requires very skilled technicians to write. This has made it very difficult for threat actors with a small footprint in the cyber domain to create and carry out ransomware attacks. However, ransomware attacks provide threat actors with a quick payday to re-invest in their operations, making the attack vector highly sought after. Therefore, large threat actors within the domain established RaaS operations. This provides all threat actors with the ability to buy the rights to use the ransomware at a fraction of the resources it takes to create the source code. Over the past two years, major cyber threat actors have had their ransomware source code leaked, or ex-hackers have left one organization and brought source code to their new employer.

The trend of several organizations using the same granular TTPs can pose a significant threat as these operations often enable more sophisticated and successful attacks than would be possible as separate entities. Additionally, the collaboration between threat actors also broadens the ability to target several industries. These incidents of cluster activity suggest that there is a trend toward a greater democratization of ransomware adversaries.

Read More for Risks & Mitigations

Top 3 Malware

Threat: QatBot, SocGholish, Raspberry Robin, Redline, Remcos, njRA

Type of Threat: Malware loaders and malware

Targeted Industries: All Industries

The enduring and evolving menace of malware remains a paramount concern within the cybersecurity realm, posing a threat to individuals, organizations, and even entire nations. Malware employs various entry points to infiltrate systems, ranging from malicious email attachments and compromised websites to sophisticated social engineering tactics that deceive unsuspecting users into executing malicious code. Simultaneously, malware creators continue to refine their techniques, incorporating polymorphic malware and advanced evasion strategies to evade detection.

The financial ramifications of malware attacks are profoundly significant, casting a formidable shadow over both businesses and individuals. These consequences encompass a range of financial burdens, including the costly endeavor of data recovery, legal expenses, regulatory penalties, and the damaging impact on reputation. Beyond the realm of financially motivated cybercrime, the specter of state-sponsored malware looms large, targeting critical infrastructure and government entities and amplifying the multifaceted nature of malware threats.

The malware landscape in 2023 presents substantial challenges for both individuals and organizations. It is characterized by the dominance of three versatile malware loaders—QakBot, SocGholish, and Raspberry Robin. These cyber threats encompass a wide spectrum of dangers, including ransomware, viruses, trojans, and worms. The adaptability of these malicious actors enables them to target various industries and regions, contributing to a complex and ever-evolving cybersecurity landscape.

Read More for Risks & Mitigations

Top 10 Threats of H2 2023

Malicious QR Codes

Threat: Malicious QR Codes

Type of Threat: Phishing campaign

Targeted Industries: Energy

Since May 2023, a large phishing campaign has been utilizing Quick Response (**QR**) codes in an attempt to collect Microsoft credentials from victims. The emails masquerade as a Microsoft security notification with a QR code embedded inside a PNG image or a PDF attachment. This phishing campaign has been seen across multiple industries, with the energy sector being the largest industry targeted. A US-based energy company has been the primary target, receiving 29% of the emails pertaining to this phishing campaign. Other top industries targeted include manufacturing, insurance, technology, and financial services. Most of the QR codes send individuals to a Bing redirect URL; however, other domains, such as krxd[.]com (associated with the Salesforce application), and cf-ipfs[.]com (Cloudflare's Web3 services) have also been used. This phishing campaign marks a shift in threat actor tactics, as QR codes have traditionally not been used in phishing attacks.

Read More for Risks & Mitigations

Domino Malware

Threat: Domino

Type of Threat: Malware

Targeted Industries: All Industries

Domino (aka Minodo) is a new malware family that consists of two components, the Domino Backdoor and Domino Loader, which was first discovered being used in the fall of 2022. The Domino Backdoor collects system information, such as running processes, usernames, and computer names, and then proceeds to send this information to the attacker's command-and-control server. Once contact is made with the command-and-control server the threat actor sends commands to install Domino Loader. The Domino Loader is being used to deliver the final payload of an information-stealer called Project Nemesis. It is assessed that Project Nemesis is being used by ex-Conti hackers to collect data from a range of web browsers and applications, including Steam, Telegram, Discord, crypto wallets, and VPN providers.

Domino malware is still relatively new, and while it currently only drops Cobalt Strike or Project Nemesis, it is possible that the malware will be updated to drop other malware developed by FIN7 in the future. It is highly likely that FIN7 will continue to package their developed malware to sell to other organizations to increase the group's profits. Collaboration between different cyber threat groups highlights the complex and ever-changing nature of the cybercrime economy. Organizations must remain vigilant and adopt robust security measures, including predictive DNS technology, to mitigate the risk of being targeted by sophisticated cyber-attacks.

Read More for Risks & Mitigations

Top 10 Threats of H2 2023

Volt Typhoon

Threat: Volt Typhoon

Type of Threat: Advanced Persistent Threat (**APT**) group conducting espionage operations

Targeted Industries: All Industries Critical Infrastructure, Education, Government, Real Estate & Construction, Software & IT, Transportation

Volt Typhoon, a threat actor sponsored by the Chinese state, is employing stealth techniques in its cyber espionage operations targeting government and critical infrastructure entities. Recent attacks by Volt Typhoon have involved application and server-side exploits to gain initial entry into victims' networks. Utilizing built-in network administration tools and hands-on keyboard actions, Volt Typhoon adeptly camouflages its actions as routine system and network operations to avoid detection. This sophisticated threat poses a significant risk to national security and critical infrastructure organizations. Given their propensity for stealth and advanced tactics, Volt Typhoon is likely to persist in carrying out cyber espionage campaigns to support the broader Chinese government agenda against U.S. critical infrastructure. It is imperative for government and critical infrastructure entities to maintain vigilance against Volt Typhoon's activities. Strengthening threat detection, monitoring, and response capabilities is essential to effectively counter their evolving tactics. Collaborative efforts with international partners and security communities can enhance information sharing and enable timely responses to mitigate the impact of Volt Typhoon's cyber espionage operations.

Read More for Risks & Mitigations

Kubernetes Clusters

Threat: Exploitation Kubernetes Role-Based Access Control (**RBAC**)

Type of Threat: Cryptocurrency mining campaign

Targeted Industries: All Industries

A significant cryptocurrency mining campaign, known as RBAC Buster, has been detected actively targeting a minimum of 60 Kubernetes clusters in the wild. This campaign exploits vulnerabilities in Kubernetes RBAC to establish illicit backdoors and initiate cryptocurrency mining operations. The attackers capitalized on a misconfigured API server to gain initial entry into these clusters and subsequently employed DaemonSets to create these backdoors and carry out mining activities. The cybersecurity firm Aqua Security uncovered this campaign while utilizing Kubernetes honeypots and exposing Amazon Web Services (**AWS**) access keys within various cluster locations. To fortify Kubernetes environments, organizations must implement customizable Identity and Access Management (**IAM**) solutions that delineate specific roles and permissions for individual users. Authorization levels should be precisely defined based on user types, with corresponding access rules established. IAM serves as the means to authenticate individuals, while native Kubernetes RBACs may necessitate adjustments for effective management.

Organizations should adopt a principle of least privilege, granting only the minimum necessary level of access when creating roles for different user groups. Roles that are no longer required should be promptly deleted. IAM solutions can streamline the process of configuring, managing, and ensuring the scalability of clusters while correctly assigned roles persist as a crucial layer of security. As Kubernetes continues to evolve and expand in usage, security measures will adapt, but the careful specification of roles will remain an enduring cornerstone of its security framework.

Read More for Risks & Mitigations

Protecting your Organization

Critical Start's Managed Detection and Response (MDR) and CTI Services

To further enhance your protection against these emerging and evolving threats, organizations should consider 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 MDR services, powered by our **Cyber Operations Risk & Response™ platform**, 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 RSOC guarantees contractual SLAs of 60-minute or less Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) for all alerts, regardless of priority. 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.

About Critical Start CTI

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 RSOC 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/cyber-research-unit

© 2023 CRITICALSTART. All rights reserved.