Co-authored by:

Product ID: AA23-025A

January 25, 2023

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Protecting Against Malicious Use of Remote Monitoring and Management Software

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the "authoring organizations") are releasing this joint Cybersecurity Advisory (CSA) to warn network defenders about malicious use of legitimate remote monitoring and management (RMM) software. In October 2022, CISA identified a widespread cyber campaign involving the malicious use of legitimate RMM software. Specifically, cyber criminal actors sent phishing emails that led to the download of legitimate RMM software—ScreenConnect (now ConnectWise Control) and AnyDesk—which the actors used in a refund scam to steal money from victim bank accounts.

Although this campaign appears financially motivated, the authoring organizations assess it could lead to additional types of malicious activity. For example, the actors could sell victim account access to other cyber criminal or advanced persistent threat (APT) actors. This campaign highlights the threat of malicious cyber activity associated with legitimate RMM software: after gaining access to the target network via phishing or other techniques, malicious cyber actors—from cybercriminals to nation-state sponsored APTs—are known to use legitimate RMM software as a backdoor for persistence and/or command and control (C2).

Using portable executables of RMM software provides a way for actors to establish local user access without the need for administrative privilege and full software installation—effectively bypassing common software controls and risk management assumptions.

The authoring organizations strongly encourage network defenders to review the Indicators of Compromise (IOCs) and Mitigations sections in this CSA and apply the recommendations to protect against malicious use of legitimate RMM software.

All organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov. State, local, tribal, and territorial government entities can also report to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

For a downloadable copy of IOCs, see AA23-025.stix (STIX, 19 kb).

TECHNICAL DETAILS

Overview

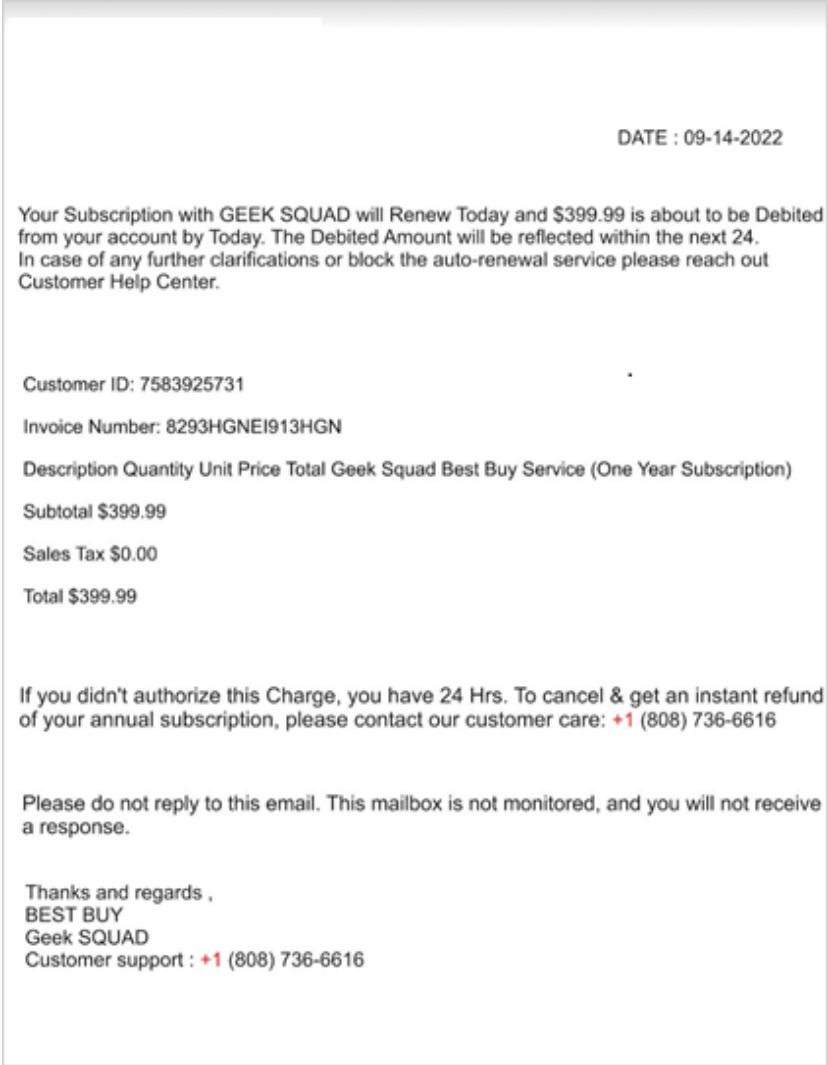
In October 2022, CISA used trusted third-party reporting, to conduct retrospective analysis of EINSTEIN—a federal civilian executive branch (FCEB)-wide intrusion detection system (IDS) operated and monitored by CISA—and identified suspected malicious activity on two FCEB networks:

- In mid-June 2022, malicious actors sent a phishing email containing a phone number to an FCEB employee's government email address. The employee called the number, which led them to visit the malicious domain, `myhelpcare[.]online`.
- In mid-September 2022, there was bi-directional traffic between an FCEB network and `myhelpcare[.]cc`.

Based on further EINSTEIN analysis and incident response support, CISA identified related activity on many other FCEB networks. The authoring organizations assess this activity is part of a widespread, financially motivated phishing campaign and is related to malicious typosquatting activity reported by Silent Push in the blog post Silent Push uncovers a large trojan operation featuring Amazon, Microsoft, Geek Squad, McAfee, Norton, and Paypal domains.

Malicious Cyber Activity

The authoring organizations assess that since at least June 2022, cyber criminal actors have sent help desk-themed phishing emails to FCEB federal staff's personal, and government email addresses. The emails either contain a link to a "first-stage" malicious domain or prompt the recipients to call the cybercriminals, who then try to convince the recipients to visit the first-stage malicious domain. See figure 1 for an example phishing email obtained from an FCEB network.



DATE : 09-14-2022

Your Subscription with GEEK SQUAD will Renew Today and $399.99 is about to be Debited from your account by Today. The Debited Amount will be reflected within the next 24.
In case of any further clarifications or block the auto-renewal service please reach out Customer Help Center.

Customer ID: 7583925731

Invoice Number: 8293HGNEI913HGN

Description Quantity Unit Price Total Geek Squad Best Buy Service (One Year Subscription)

Subtotal $399.99

Sales Tax $0.00

Total $399.99

If you didn't authorize this Charge, you have 24 Hrs. To cancel & get an instant refund of your annual subscription, please contact our customer care: +1 (808) 736-6616

Please do not reply to this email. This mailbox is not monitored, and you will not receive a response.

Thanks and regards ,
BEST BUY
Geek SQUAD
Customer support : +1 (808) 736-6616

Figure 1: Help desk-themed phishing email example

The recipient visiting the first-stage malicious domain triggers the download of an executable. The executable then connects to a "second-stage" malicious domain, from which it downloads additional RMM software.

CISA noted that the actors did not install downloaded RMM clients on the compromised host. Instead, the actors downloaded AnyDesk and ScreenConnect as self-contained, portable executables configured to connect to the actor's RMM server.

Note: Portable executables launch within the user's context without installation. Because portable executables do not require administrator privileges, they can allow execution of unapproved software even if a risk management control may be in place to audit or block the same software's installation on the network. Threat actors can leverage a portable executable with local user rights to attack other vulnerable machines within the local intranet or establish long term persistent access as a local user service.

CISA has observed that multiple first-stage domain names follow naming patterns used for IT help/support themed social-engineering, e.g., `hservice[.]live`, `gscare[.]live`, `nhelpcare[.]info`, `deskcareme[.]live`, `nhelpcare[.]cc`). According to Silent Push, some of these malicious domains impersonate known brands such as, Norton, GeekSupport, Geek Squad, Amazon, Microsoft, McAfee, and PayPal.[1] CISA has also observed that the first-stage malicious domain linked in the initial phishing email periodically redirects to other sites for additional redirects and downloads of RMM software.

Use of Remote Monitoring and Management Tools

In this campaign, after downloading the RMM software, the actors used the software to initiate a refund scam. They first connected to the recipient's system and enticed the recipient to log into their bank account while remaining connected to the system. The actors then used their access through the RMM software to modify the recipient's bank account summary. The falsely modified bank account summary showed the recipient was mistakenly refunded an excess amount of money. The actors then instructed the recipient to "refund" this excess amount to the scam operator.

Although this specific activity appears to be financially motivated and targets individuals, the access could lead to additional malicious activity against the recipient's organization—from both other cybercriminals and APT actors. Network defenders should be aware that:

- Although the cybercriminal actors in this campaign used ScreenConnect and AnyDesk, threat actors can maliciously leverage any legitimate RMM software.
- Because threat actors can download legitimate RMM software as self-contained, portable executables, they can bypass both administrative privilege requirements and software management control policies.
- The use of RMM software generally does not trigger antivirus or antimalware defenses.
- Malicious cyber actors are known to leverage legitimate RMM and remote desktop software as backdoors for persistence and for C2.[2],[3],[4],[5],[6],[7],[8]
- RMM software allows cyber threat actors to avoid using custom malware.

Threat actors often target legitimate users of RMM software. Targets can include managed service providers (MSPs) and IT help desks, who regularly use legitimate RMM software for technical and security end-user support, network management, endpoint monitoring, and to interact remotely with hosts for IT-support functions. These threat actors can exploit trust relationships in MSP networks and gain access to a large number of the victim MSP's customers. MSP compromises can introduce significant risk—such as ransomware and cyber espionage—to the MSP's customers.

The authoring organizations strongly encourage network defenders to apply the recommendations in the Mitigations section of this CSA to protect against malicious use of legitimate RMM software.

INDICATORS OF COMPROMISE

See table 1 for IOCs associated with the campaign detailed in this CSA.

Table 1: Malicious Domains and IP addresses observed by CISA

Domain	Description	Date(s) Observed
win03[.]xyz	Suspected first-stage malware domain	June 1, 2022 July 19, 2022
myhelpcare[.]online	Suspected first-stage malware domain	June 14, 2022
win01[.]xyz	Suspected first-stage malware domain	August 3, 2022 August 18, 2022
myhelpcare[.]cc	Suspected first-stage malware domain	September 14, 2022
247secure[.]us	Second-stage malicious domain	October 19, 2022 November 10, 2022

Additional resources to detect possible exploitation or compromise:

- Silent Push: Silent Push uncovers a large trojan operation featuring Amazon, Microsoft, Geek Squad, McAfee, Norton, and Paypal domains.

MITIGATIONS

The authoring organizations encourage network defenders to:

- Implement best practices to block phishing emails. See CISA's Phishing Infographic for more information.
- Audit remote access tools on your network to identify currently used and/or authorized RMM software.
- Review logs for execution of RMM software to detect abnormal use of programs running as a portable executable.
- Use security software to detect instances of RMM software only being loaded in memory.
- Implement application controls to manage and control execution of software, including allowlisting RMM programs.
    - See NSA Cybersecurity Information sheet Enforce Signed Software Execution Policies.
    - Application controls should prevent both installation and execution of portable versions of unauthorized RMM software.
- Require authorized RMM solutions only be used from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
- Block both inbound and outbound connections on common RMM ports and protocols at the network perimeter.
- Implement a user training program and phishing exercises to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.

RESOURCES

- See CISA Insights Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses for guidance on hardening MSP and customer infrastructure.
- U.S. Defense Industrial Base (DIB) Sector organizations may consider signing up for the NSA Cybersecurity Collaboration Center's DIB Cybersecurity Service Offerings, including Protective Domain Name System (PDNS) services, vulnerability scanning, and threat intelligence collaboration for eligible organizations. For more information on how to enroll in these services, email dib_defense@cyber.nsa.gov.
- CISA offers several Vulnerability Scanning to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. See cisa.gov/cyber-hygiene-services.
- Consider participating in CISA's Automated Indicator Sharing (AIS) to receive real-time exchange of machine-readable cyber threat indicators and defensive measures. AIS is offered at no cost to participants as part of CISA's mission to work with our public and private sector

partners to identify and help mitigate cyber threats through information sharing and provide technical assistance, upon request, that helps prevent, detect, and respond to incidents.

REFERENCES

[1] Silent Push uncovers a large trojan operation featuring Amazon, Microsoft, Geek Squad, McAfee, Norton, and Paypal domains. — Silent Push Threat Intelligence

[2] Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization | CISA

[3] Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks | CISA

[4] Karakurt Data Extortion Group | CISA

[5] Compromise of U.S. Water Treatment Facility | CISA

[6] North Korean Advanced Persistent Threat Focus: Kimsuky | CISA

[7] Continued Threat Actor Exploitation Post Pulse Secure VPN Patching | CISA

[8] FBI Warns Public to Beware of Tech Support Scammers Targeting Financial Accounts Using Remote Desktop Software — FBI

PURPOSE

This advisory was developed by CISA, NSA, and MS-ISAC in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA, NSA, and MS-ISAC do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring.