Phishing Emails Used to Deploy KONNI Malware

us-cert.cisa.gov/ncas/alerts/aa20-227a

Summary

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) has observed cyber actors using emails containing a Microsoft Word document with a malicious Visual Basic Application (VBA) macro code to deploy KONNI malware. KONNI is a remote administration tool (RAT) used by malicious cyber actors to steal files, capture keystrokes, take screenshots, and execute arbitrary code on infected hosts.

Technical Details

KONNI malware is often delivered via phishing emails as a Microsoft Word document with a malicious VBA macro code (*Phishing: Spearphising Attachment* [T1566.001]). The malicious code can change the font color from light grey to black (to fool the user to enable content), check if the Windows operating system is a 32-bit or 64-bit version, and construct and execute the command line to download additional files (*Command and Scripting Interpreter: Windows Command Shell* [T1059.003]).

Once the VBA macro constructs the command line, it uses the certificate database tool CertUtil to download remote files from a given Uniform Resource Locator. It also incorporates a built-in function to decode base64-encoded files. The Command Prompt silently copies `certutil.exe` into a temp directory and renames it to evade detection.

The cyber actor then downloads a text file from a remote resource containing a base64-encoded string that is decoded by CertUtil and saved as a batch (.BAT) file. Finally, the cyber actor deletes the text file from the temp directory and executes the .BAT file.

MITRE ATT&CK Techniques

According to MITRE, KONNI uses the ATT&CK techniques listed in table 1.

Table 1: KONNI ATT&CK techniques

Technique	Use

Technique	Use
System Network Configuration Discovery [T1016]	KONNI can collect the Internet Protocol address from the victim’s machine.
System Owner/User Discovery [T1033]	KONNI can collect the username from the victim’s machine.
Masquerading: Match Legitimate Name or Location [T1036.005]	KONNI creates a shortcut called `Anti virus service.lnk` in an apparent attempt to masquerade as a legitimate file.
Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol [T1048.003]	KONNI has used File Transfer Protocol to exfiltrate reconnaissance data out.
Input Capture: Keylogging [T1056.001]	KONNI has the capability to perform keylogging.
Process Discovery [T1057]	KONNI has used `tasklist.exe` to get a snapshot of the current processes’ state of the target machine.
Command and Scripting Interpreter: PowerShell [T1059.001]	KONNI used PowerShell to download and execute a specific 64-bit version of the malware.
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	KONNI has used `cmd.exe` to execute arbitrary commands on the infected host across different stages of the infection change.
Indicator Removal on Host: File Deletion [T1070.004]	KONNI can delete files.
Application Layer Protocol: Web Protocols [T1071.001]	KONNI has used Hypertext Transfer Protocol for command and control.

Technique	Use
System Information Discovery [T1082]	KONNI can gather the operating system version, architecture information, connected drives, hostname, and computer name from the victim's machine and has used `systeminfo.exe` to get a snapshot of the current system state of the target machine.
File and Directory Discovery [T1083]	A version of KONNI searches for filenames created with a previous version of the malware, suggesting different versions targeted the same victims and the versions may work together.
Ingress Tool Transfer [T1105]	KONNI can download files and execute them on the victim's machine.
Modify Registry [T1112]	KONNI has modified registry keys of ComSysApp service and Svchost on the machine to gain persistence.
Screen Capture [T1113]	KONNI can take screenshots of the victim's machine.
Clipboard Data [T1115]	KONNI had a feature to steal data from the clipboard.
Data Encoding: Standard Encoding [T1132.001]	KONNI has used a custom base64 key to encode stolen data before exfiltration.
Access Token Manipulation: Create Process with Token [T1134.002]	KONNI has duplicated the token of a high integrity process to spawn an instance of cmd.exe under an impersonated user.
Deobfuscate/Decode Files or Information [T1140]	KONNI has used CertUtil to download and decode base64 encoded strings.
Signed Binary Proxy Execution: Rundll32 [T1218.011]	KONNI has used Rundll32 to execute its loader for privilege escalation purposes.

Technique	Use
Event Triggered Execution: Component Object Model Hijacking [T1546.015]	KONNI has modified ComSysApp service to load the malicious DLL payload.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	A version of KONNI drops a Windows shortcut into the Startup folder to establish persistence.
Boot or Logon Autostart Execution: Shortcut Modification [T1547.009]	A version of KONNI drops a Windows shortcut on the victim's machine to establish persistence.
Abuse Elevation Control Mechanism: Bypass User Access Control [T1548.002]	KONNI bypassed User Account Control with the "AlwaysNotify" settings.
Credentials from Password Stores: Credentials from Web Browsers [T1555.003]	KONNI can steal profiles (containing credential information) from Firefox, Chrome, and Opera.

Detection

Signatures

CISA developed the following Snort signatures for use in detecting KONNI malware exploits.

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP URI contains '/weget/*.php'
(KONNI)"; sid:1; rev:1; flow:established,to_server; content:"/weget/";
http_uri; depth:7; offset:0; fast_pattern; content:".php"; http_uri;
distance:0; within:12; content:!"Referrer|3a 20|"; http_header;
classtype:http-uri; priority:2; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"KONNI:HTTP header contains
'User-Agent|3a 20|HTTP|0d 0a|'"; sid:1; rev:1; flow:established,to_server;
content:"User-Agent|3a 20|HTTP|0d 0a|"; http_header; fast_pattern:only;
content:"POST"; nocase; http_method; classtype:http-header; priority:2;
metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"KONNI:HTTP URI contains
'/weget/(upload|uploadtm|download)'"; sid:1; rev:1;
flow:established,to_server; content:"/weget/"; http_uri; fast_pattern:only;
pcre:"/^\/weget\x2f(?:upload|uploadtm|download)\.php/iU"; content:"POST";
http_method; classtype:http-uri; priority:2;
reference:url,blog.talosintelligence.com/2017/07/konni-references-north-
korean-missile-capabilities.html; metadata:service http;)
```

Mitigations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines. See Protecting Against Malicious Code.
- Keep operating system patches up to date. See Understanding Patches and Software Updates.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators’ group unless required.
- Enforce a strong password policy. See Choosing and Protecting Passwords.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Visit the MITRE ATT&CK Techniques pages (linked in table 1 above) for additional mitigation and detection strategies.

For additional information on malware incident prevention and handling, see the National Institute of Standards and Technology Special Publication 800-83, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops."

Resources

Revisions

August 14, 2020: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.