



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

CYBERSECURITY ADVISORY

Phishing Emails Used to Deploy KONNI Malware

Last Revised: October 24, 2020

Alert Code: AA20-227A

Summary

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the [ATT&CK for Enterprise](#)

<<https://attack.mitre.org/versions/v7/matrices/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: Spearphishing Attachment* [T1566.001 <<https://attack.mitre.org/versions/v7/techniques/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 <<https://attack.mitre.org/versions/v7/techniques/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 <<https://attack.mitre.org/versions/v7/software/s0356/>> uses the ATT&CK techniques listed in table 1.

Table 1: KONNI ATT&CK techniques

Technique	Use
System Network Configuration Discovery [T1016 < https://attack.mitre.org/versions/v7/techniques/t1016/ >]	KONNI can collect the Internet Protocol address from the victim's machine.

Give Feedback

Technique	Use
<p><i>System Owner/User Discovery</i> [T1033 <https://attack.mitre.org/versions/v7/techniques/t1033>]</p>	<p>KONNI can collect the username from the victim's machine.</p>
<p><i>Masquerading: Match Legitimate Name or Location</i> [T1036.005 <https://attack.mitre.org/versions/v7/techniques/t1036/005>]</p>	<p>KONNI creates a shortcut called <code>Anti virus service.lnk</code> in an apparent attempt to masquerade as a legitimate file.</p>
<p><i>Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol</i> [T1048.003 <https://attack.mitre.org/versions/v7/techniques/t1048/003>]</p>	<p>KONNI has used File Transfer Protocol to exfiltrate reconnaissance data out.</p>
<p><i>Input Capture: Keylogging</i> [T1056.001 <https://attack.mitre.org/versions/v7/techniques/t1056/001>]</p>	<p>KONNI has the capability to perform keylogging.</p>
<p><i>Process Discovery</i> [T1057 <https://attack.mitre.org/versions/v7/techniques/t1057>]</p>	<p>KONNI has used <code>tasklist.exe</code> to get a snapshot of the current processes' state of the target machine.</p>
<p><i>Command and Scripting Interpreter: PowerShell</i> [T1059.001 <https://attack.mitre.org/versions/v7/techniques/t1059/001>]</p>	<p>KONNI used PowerShell to download and execute a specific 64-bit version of the malware.</p>
<p><i>Command and Scripting Interpreter: Windows Command Shell</i> [T1059.003 <https://attack.mitre.org/versions/v7/techniques/t1059/003>]</p>	<p>KONNI has used <code>cmd.exe</code> to execute arbitrary commands on the infected host across different stages of the infection change.</p>

Technique	Use
<i>Indicator Removal on Host: File Deletion</i> [T1070.004 https://attack.mitre.org/versions/v7/techniques/t1070/004]	KONNI can delete files.
<i>Application Layer Protocol: Web Protocols</i> [T1071.001 https://attack.mitre.org/versions/v7/techniques/t1071/001]	KONNI has used Hypertext Transfer Protocol for command and control.
<i>System Information Discovery</i> [T1082 https://attack.mitre.org/versions/v7/techniques/t1082]	KONNI can gather the operating system version, architecture information, connected drives, hostname, and computer name from the victim's machine and has used <code>systeminfo.exe</code> to get a snapshot of the current system state of the target machine.
<i>File and Directory Discovery</i> [T1083 https://attack.mitre.org/versions/v7/techniques/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.
<i>Ingress Tool Transfer</i> [T1105 https://attack.mitre.org/versions/v7/techniques/t1105]	KONNI can download files and execute them on the victim's machine.
<i>Modify Registry</i> [T1112 https://attack.mitre.org/versions/v7/techniques/t1112]	KONNI has modified registry keys of ComSysApp service and Svchost on the machine to gain persistence.

Technique	Use
Screen Capture [T1113] https://attack.mitre.org/versions/v7/techniques/t1113	KONNI can take screenshots of the victim's machine.
Clipboard Data [T1115] https://attack.mitre.org/versions/v7/techniques/t1115	KONNI had a feature to steal data from the clipboard.
Data Encoding: Standard Encoding [T1132.001] https://attack.mitre.org/versions/v7/techniques/t1132/001	KONNI has used a custom base64 key to encode stolen data before exfiltration.
Access Token Manipulation: Create Process with Token [T1134.002] https://attack.mitre.org/versions/v7/techniques/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] https://attack.mitre.org/versions/v7/techniques/t1140	KONNI has used CertUtil to download and decode base64 encoded strings.
Signed Binary Proxy Execution: Rundll32 [T1218.011] https://attack.mitre.org/versions/v7/techniques/t1218/011	KONNI has used Rundll32 to execute its loader for privilege escalation purposes.
Event Triggered Execution: Component Object Model Hijacking [T1546.015] https://attack.mitre.org/versions/v7/techniques/t1546/015	KONNI has modified ComSysApp service to load the malicious DLL payload.

Technique	Use
<i>Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder</i> [T1547.001] https://attack.mitre.org/versions/v7/techniques/t1547/001	A version of KONNI drops a Windows shortcut into the Startup folder to establish persistence.
<i>Boot or Logon Autostart Execution: Shortcut Modification</i> [T1547.009] https://attack.mitre.org/versions/v7/techniques/t1547/009	A version of KONNI drops a Windows shortcut on the victim's machine to establish persistence.
<i>Abuse Elevation Control Mechanism: Bypass User Access Control</i> [T1548.002] https://attack.mitre.org/versions/v7/techniques/t1548/002	KONNI bypassed User Account Control with the "AlwaysNotify" settings.
<i>Credentials from Password Stores: Credentials from Web Browsers</i> [T1555.003] https://attack.mitre.org/versions/v7/techniques/t1555/003	KONNI can steal profiles (containing credential information) from Firefox, Chrome, and Opera.

Give Feedback

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;)
```

Give Feedback

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](#) <<https://us-cert.cisa.gov/ncas/tips/st04-006>>.

- Disable file and printer sharing services. If these services are required, use [strong passwords](https://us-cert.cisa.gov/ncas/tips/st04-002) <<https://us-cert.cisa.gov/ncas/tips/st04-002>> 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](https://us-cert.cisa.gov/ncas/tips/st04-002) <<https://us-cert.cisa.gov/ncas/tips/st04-002>>.
- 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.

Give Feedback

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](https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final)" <<https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final>>."

Resources

- d-hunter – A Look Into KONNI 2019 Campaign
- MITRE ATT&CK – KONNI <<https://attack.mitre.org/versions/v7/software/s0356/>>

Revisions

August 14, 2020: Initial Version

This product is provided subject to this [Notification](#) </notification> and this [Privacy & Use](#) </privacy-policy> policy.



Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

[Return to top](#)

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>

Give Feedback



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



CISA Central

1-844-Say-CISA

contact@cisa.dhs.gov



CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Budget and Performance](#)

[DHS.gov <https://www.dhs.gov>](#)

[<https://www.dhs.gov/performance-financial-reports>](#)

[FOIA Requests](#)

[<https://www.dhs.gov/foia>](#)

[No FEAR Act </no-fear-act>](#)

[Office of Inspector General](#)

[<https://www.oig.dhs.gov/>](#)

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House](#)

[<https://www.whitehouse.gov/>](#)

[USA.gov <https://www.usa.gov/>](#)

[Website Feedback </forms/feedback>](#)

Give Feedback