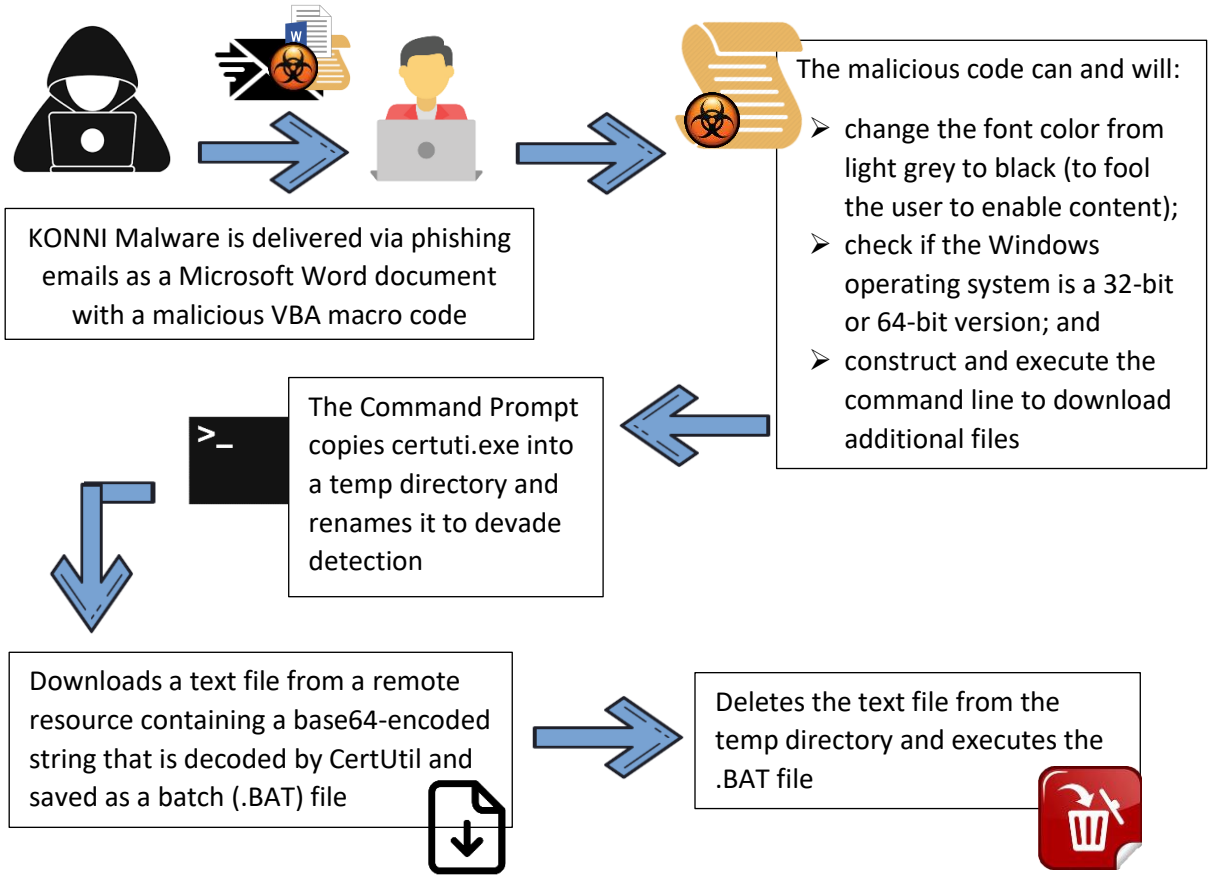
Phishing Emails Used to Deploy KONNI Malware
(CSB20-13)

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.

How it works



MITRE ATT&CK Techniques

Technique	Use
System Network Configuration Discovery	KONNI can collect the Internet Protocol address from the victim's machine
System Owner/User Discovery	KONNI can collect the username from the victim's machine.
Masquerading: Match Legitimate Name or Location	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	KONNI has used File Transfer Protocol to exfiltrate reconnaissance data out.
Input Capture: Keylogging	KONNI has the capability to perform keylogging.
Process Discovery	KONNI has used tasklist.exe to get a snapshot of the current processes' state of the target machine.
Command and Scripting Interpreter: PowerShell	KONNI used PowerShell to download and execute a specific 64-bit version of the malware.
Command and Scripting Interpreter: Windows Command Shell	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	KONNI can delete files.
Application Layer Protocol: Web Protocols	KONNI has used Hypertext Transfer Protocol for command and control.
System Information Discovery	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	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	KONNI can download files and execute them on the victim's machine.
Modify Registry	KONNI has modified registry keys of ComSysApp service and Svchost on the machine to gain persistence.
Screen Capture	KONNI can take screenshots of the victim's machine.
Clipboard Data	KONNI had a feature to steal data from the clipboard.
Data Encoding: Standard Encoding	KONNI has used a custom base64 key to encode stolen data before exfiltration.

Access Token Manipulation: Create Process with Token	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	KONNI has used CertUtil to download and decode base64 encoded strings.
Signed Binary Proxy Execution: Rundll32	KONNI has used Rundll32 to execute its loader for privilege escalation purposes.
Event Triggered Execution: Component Object Model Hijacking	KONNI has modified ComSysApp service to load the malicious DLL payload.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	A version of KONNI drops a Windows shortcut into the Startup folder to establish persistence.
Boot or Logon Autostart Execution: Shortcut Modification	A version of KONNI drops a Windows shortcut on the victim's machine to establish persistence.
Abuse Elevation Control Mechanism: Bypass User Access Control	KONNI bypassed User Account Control with the "AlwaysNotify" settings.
Credentials from Password Stores: Credentials from Web Browsers	KONNI can steal profiles (containing credential information) from Firefox, Chrome, and Opera.

DETECTION

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

- Maintain up-to-date antivirus signatures and engines;
- Keep operating system patches up to date;
- 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;
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known;
- 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; and
- Maintain situational awareness of the latest threats and implement appropriate access control lists.

REFERENCE

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