Mphasis

The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 24-06-2024, 11:30 IST

Title	SmallTiger Malware Used in Attacks Against South Korean Businesses (Kimsuky and Andariel)
Summary	A malware campaign distributing SmallTiger malware has been reported targeting Korean companies in the defense, automobile parts, and semiconductor manufacturing sectors. This malware acts as a downloader, connecting to the attackers' C&C server to fetch and execute the final payload in memory. As part of the attack chain, the attackers install Mimikatz and ProcDump on the compromised systems. The ProcDump tool is used to dump the memory of the LSASS process, thereby stealing credentials from the infected systems. Additionally, a command-line tool is utilized to extract and display account information and web browser history.
Severity	Medium
Attack Vectors	• Since February 2024, there have been confirmed cases in which the same threat actor abused different software in their attack. The malware in the form of DLL is installed during the internal propagation phase. It is a downloader that accesses the C&C server to download a payload and executes it inside the memory. The downloader malware in this case is classified as SmallTiger based on the name of the DLL given by the developer (threat actor). • The threat actor also installed Mimikatz and ProcDump during the infiltration stage and dumped the memory of the LSASS process using the ProcDump tool to hijack the infected system's credentials. • In this case, the malware that steals the information from NirSoft's WebBrowserPassView and web browser was also discovered. It is a command line tool like WebBrowserPassView in that it extracts and shows the account and history information saved in Google Chrome, Firefox, and Internet Explorer. • Unlike in November 2023 where the threat actor used a dropper that creates DurianBeacon, a downloader with the same name (j******n.exe) was used in April 2024. The malware downloads a malicious JavaScript from the C&C server using the mshta command and runs it. The downloaded JavaScript creates a payload that is included internally at the "C:/Users/Public/printsys.dll: mdata" path—the alternate data stream (ADS) area—and runs it using rundll32. As a result, SmallTiger is created. • In May 2024, GitHub was used instead of the usual C&C server to distribute SmallTiger. "pk.dll" is the file that is installed at the end, and it is the SmallTiger malware just like the past attack cases.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	2b8fabd12a20fd4a6b5b426dca916f68 1210ff921922f2e27db4feae9fe63394 e930b05efe23891d19bc354a4209be3e 57445041f7a1e57da92e858fc3efeabe 57445041f7a1e57da92e858fc3efeabe 48d53985cefb9029feb349bcd514c444
	IP address	• 104.168.145[.]83 • 38.110.1[.]69:993
	URL	• Hxxp[:]//my.shoping.kro[.]kr/setting.dat • Hxxp[:]//my.shoping.kro[.]kr/m.dat hxxp://my.shoping.kro[.]kr/ng.db • Hxxp[:]//91.228.218[.]7/ • Hxxp[:]//38.110.1[.]69/ • Hxxp[:]//www.yah00.o-r[.]kr/ • Hxxp[:]//www.navver.o-r[.]kr/ • Hxxp[:]//w3.navver.o-r[.]kr/ • Hxxp[:]//www.kepir.p-e[.]kr/ • Hxxp[:]//kevinblog.ddns[.]net/ • Hxxp[:]//104.36.229[.]179/ • Hxxp[:]//www.navver.o-r[.]kr/nav.html • Hxxp[:]//w3.navver.o-r[.]kr/bbs.html • Hxxps[:]//raw.githubusercontent[.]com/phantom5201314/google/main/nav.html • Hxxps[:]//raw.githubusercontent[.]com/phantom5201314/google/main/top.png • Hxxp[:]//104.36.229[.]179/am.dll

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Security Awareness Training: Educate employees about phishing emails, suspicious attachments, and the risks associated with downloading files from unknown sources. • Email Filtering and Scanning: Implement robust email filtering solutions that can detect and block malicious attachments or links. Regularly scan incoming emails for potential threats. • Endpoint Protection: Use advanced endpoint protection software that can identify and prevent malware execution on endpoints. Ensure that all devices are up to date with security patches. • Network Segmentation: Segment the network to limit lateral movement in case of a breach. Critical systems should be isolated from less critical ones. • Behavioral Analysis: Deploy solutions that monitor user and system behavior. Detect anomalies and unusual patterns that may indicate a compromise. • Application Whitelisting: Allow only approved applications to run on endpoints. This prevents unauthorized or malicious software from executing. • Regular Backups: Regularly back up critical data and systems. Ensure backups are stored securely and can be restored quickly if needed. **NOTE: The recommended settings/controls should be implemented after due shall be evaluated on Pre -Prod or evaluate environment before implementing. diligence and impact analysis.**
References	• https://asec.ahnlab.com/en/66546/ • https://www.broadcom.com/support/security-center/protection-bulletin/smalltiger-malware-campaign-reported-targeting-korean-companies

The information contained in this message is proprietary. It is for Mphasis and its customers only.
Copyright © 2024. All rights reserved by Mphasis.