Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Tick Launches Attack on East Asian Data-Loss Prevention Software Company

Date of Publication

March 15, 2023

Admiralty Code

A1

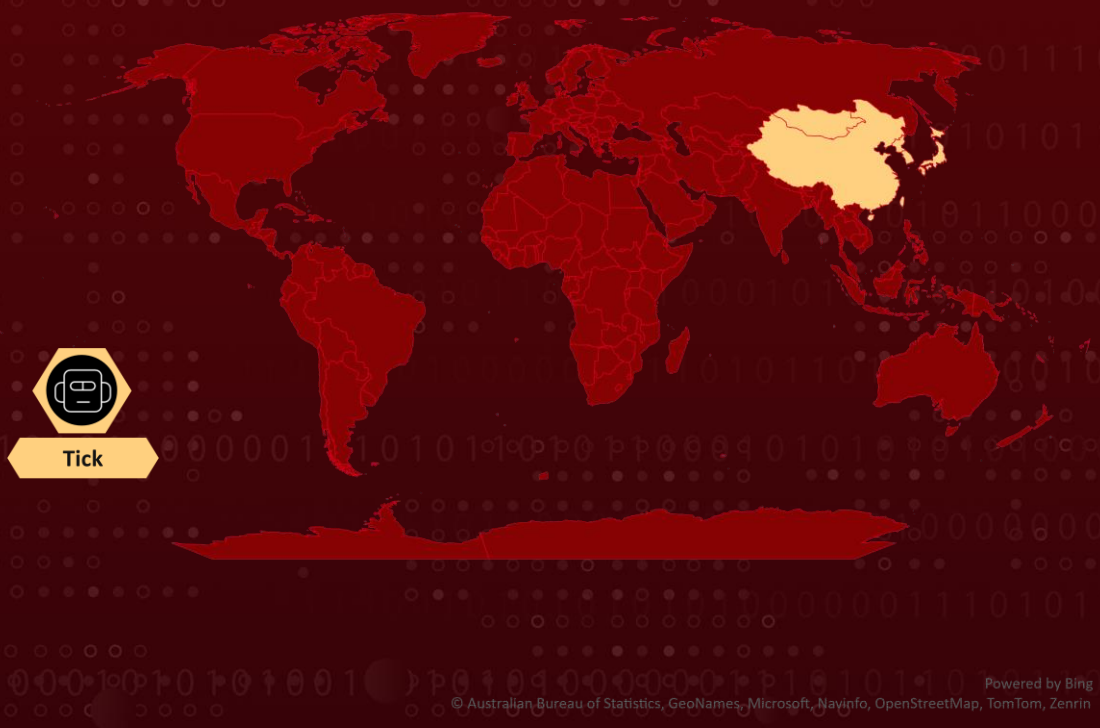
TA Number

TA2023135

Summary

Attack Begin: March 2021
Attack Region: East Asia
Attack Sector: Cybersecurity, Government, Defence
Threat Actor: Tick(BRONZE BUTLER, CTG-2006, REDBALDKNIGHT, Stalker Panda)
Malware: ShadowPy, Netboy backdoor (aka Invader), and Ghostdown downloader
Attack: Tick, an APT group, attacked an East Asian data-loss prevention software company, compromising update servers and distributing malware, using trojanized installers, to access computers of government and military entities.

Attack Regions



Attack Details

#1

The APT group, Tick, has launched a campaign against an East Asian company that develops data-loss prevention (DLP) software. The campaign involved compromising the company's internal update servers and delivering malware into the network. The attackers used trojanized installers of legitimate tools resulting in the execution of malware on the computers of the company's customers, including government and military entities. To maintain persistent access in the compromised network, Tick used several malware families, including ShadowPy, Ghostdown, and Netboy.

#2

The attackers deployed malicious loader DLLs that were vulnerable to DLL search-order hijacking. This allowed them to decode and inject a payload into a designated process. ShadowPy, a downloader developed in Python, contacted its C&C to obtain Python scripts to execute. On the other hand, Netboy, a backdoor programmed in Delphi, had multiple capabilities that allowed the attackers to capture the screen, perform mouse and keyboard events, manipulate files and services, and obtain system and network information.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1195 Supply Chain Compromise	T1195.002 Compromise Software Supply Chain	T1199 Trusted Relationship
T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1059.006 Python	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1543 Create or Modify System Process	T1543.001 Launch Agent	T1574 Hijack Execution Flow
T1574.002 DLL Side-Loading	T1036 Masquerading	T1036.004 Masquerade Task or Service	T1036.005 Match Legitimate Name or Location
T1027 Obfuscated Files or Information	T1027.001 Binary Padding	T1055 Process Injection	T1055.002 Portable Executable Injection
T1055.003 Thread Execution Hijacking	T1135 Network Share Discovery	T1120 Peripheral Device Discovery	T1057 Process Discovery
T1082 System Information Discovery	T1033 System Owner/User Discovery	T1124 System Time Discovery	T1080 Taint Shared Content
T1039 Data from Network Shared Drive	T1113 Screen Capture	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1132 Data Encoding	T1132.001 Standard Encoding	T1573 Encrypted Channel	T1041 Exfiltration Over C2 Channel
T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	72BDDEAD9B508597B75C1EE8BE970A7CA8EB85DC 8BC1F41A4DDF5CFF599570ED6645B706881BEEED 4300938A4FD4190A47EDD0D333E26C8FE2C7451E B9675D0EFBC4AE92E02B3BFC8CA04B01F8877DB6 F54F91D143399B3C9E9F7ABF0C90D60B42BF25C9 FE011D3BDF085B23E6723E8F84DD46BA63B2C700 02937E4A804F2944B065B843A31390FF958E2415
IPV4	115.144.69[.]108 110.10.16[.]56 103.127.124[.]117 103.127.124[.]119 103.127.124[.]76 58.230.118[.]78 192.185.89[.]178
Domains	travelasist[.]com mssql.waterglue[.]org slientship[.]com oracle.eneygylakes[.]com

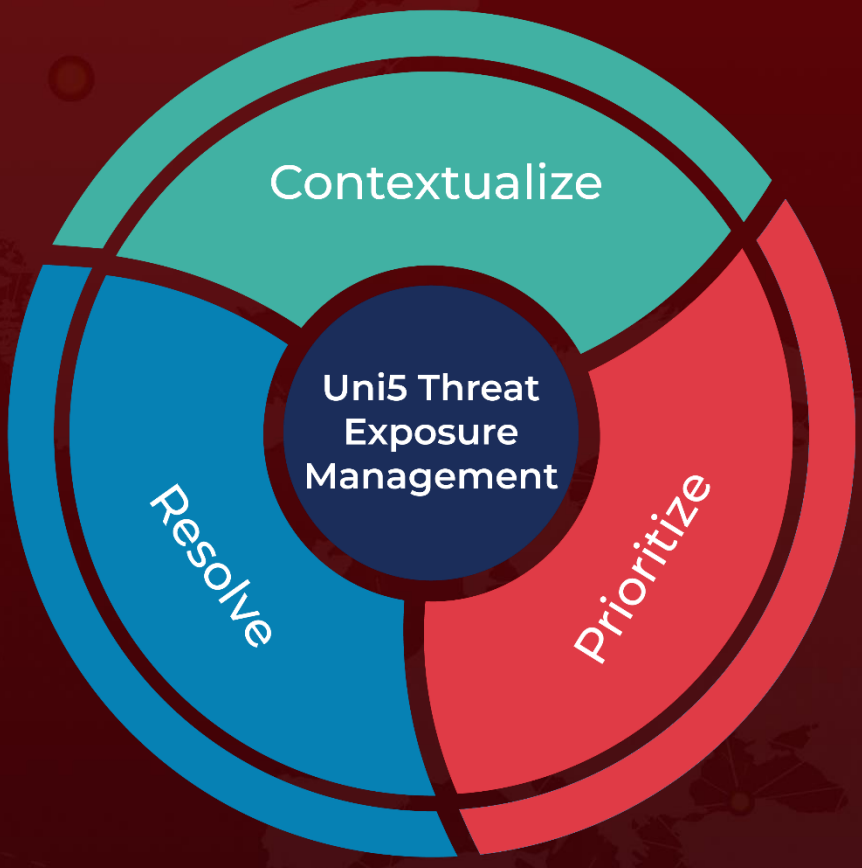
References

https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 15, 2023 • 5:00 AM

More at www.hivepro.com