MANDIANT
NOW PART OF Google Cloud

Q3 2022

Trending Evil

Based on Mandiant Managed Defense Data
from April - June 2022

Nation-State Actors Set Sights on Asia-Pacific Region

UNC

UNC2295 is suspected to be linked to APT32, an espionage operation aligned with the national interests of Vietnam. The group has targeted businesses and industries with a stake interest in the country, foreign governments, Vietnamese dissidents and journalists of interest to the ruling party of the state.

LYINGDOOR is a backdoor that is implemented as an MSBuild .NET inline task. It can execute commands, upload files from the system and download files to the system.

Managed Defense threat hunting identified and investigated intrusion activity in which victims were targeted with spear phishing through Viber and received messages with malicious links resulting in the deployment of LYINGDOOR malware.

Mandiant Managed Defense observed an increase in nation-state espionage actors targeting organizations based in Southeast Asia.

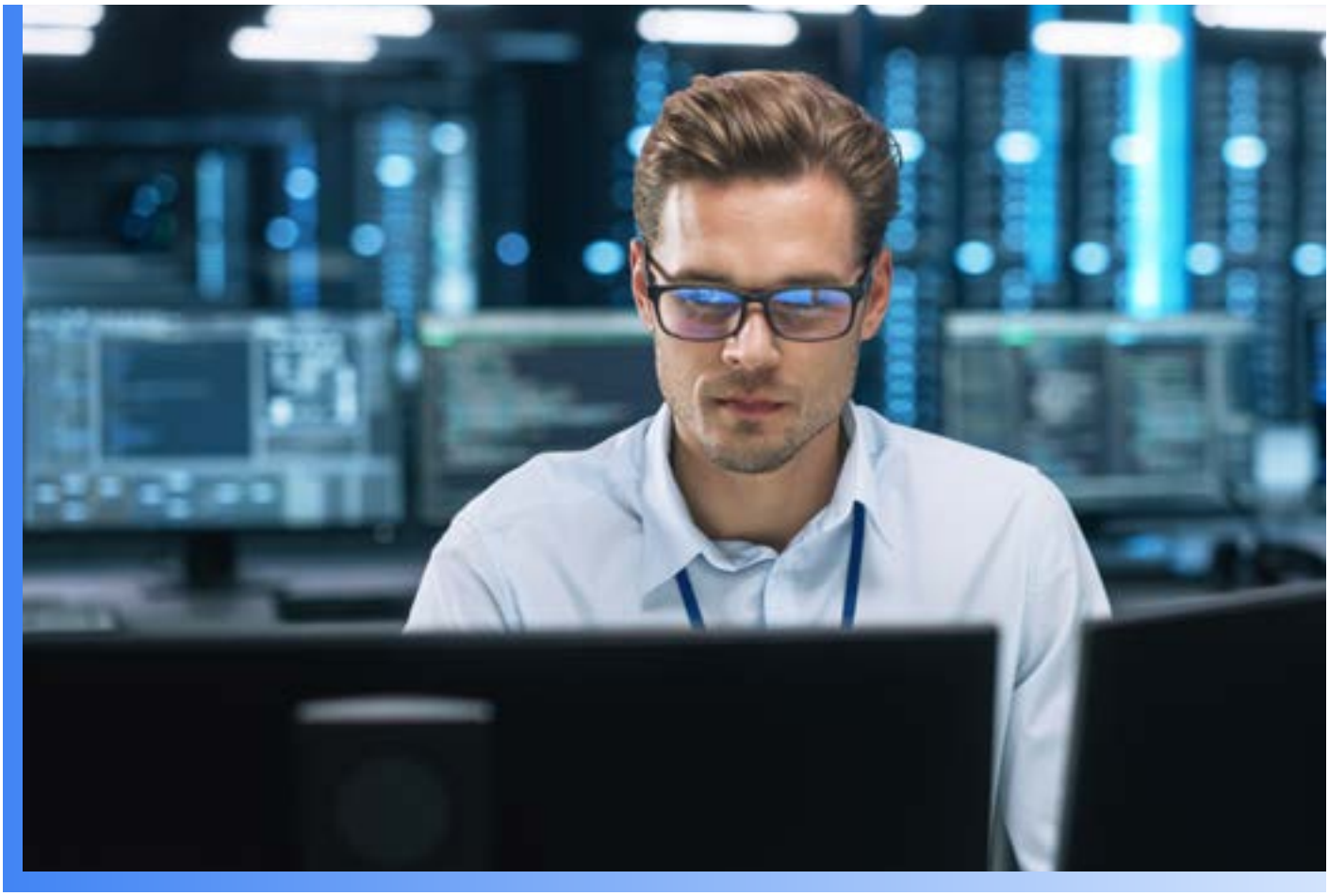
In May 2022, Managed Defense identified and responded to several campaigns attributed to UNC2295 targeting organizations located in East and Southeast Asia. Mandiant assesses with high confidence that UNC2295 is linked to APT32, an espionage operation aligned with the national interests of Vietnam.

Mandiant closely monitors threats in the region and notes this increase in cyber activity may correlate with ongoing political and economic developments, including continued efforts to attract multinational business interest in East and Southeast Asia.

Managed Defense observations are a direct result of continuous proactive hunting conducted on behalf of our customers. Several vectors leveraged by UNC2295 to gain access to environments have been uncovered, including the use of instant messaging platforms such as Viber and traditional tactics such as phishing emails to lure victims into opening and running malicious payloads. Lures identified during these campaigns include links purporting to be news articles about current regional events that, upon clicking, resulted in the deployment of LYINGDOOR malware. LYINGDOOR is a full-featured backdoor that can execute remote commands, upload files from the system and download files to the system.

Findings from Managed Defense improve detection coverage for all Mandiant customers and support the refinement of analysis and finished intelligence. Mandiant continues to track activity from UNC2295, APT32 and similar groups in reaction to geopolitical change in the region. We anticipate continued activity by UNC2295 due to Vietnam's competing interests with neighboring countries and global powers such as China and the U.S.

For further insight into APT32, see our blog citing the group's targeting of the Wuhan government in 2020 and report on APT32 activity from 2017.



BACKPUNT is a C# backdoor that supports shell execution, file upload and download. As part of its C2, BACKPUNT retrieves local system information and can communicate over SSL or over an AES encrypted binary protocol.

SHARPPUNT is a multi-stage memory-only dropper in the form of an MSBuild XML inline task file. Managed Defense discovered a new malware family, SHARPPUNT, through Network Hunting.

Two new malware families discovered

While responding to UNC2295 activity between May and June 2022, Managed Defense identified two new malware families designed to gain a foothold in compromised environments. UNC2295 used two distinct binaries to evade detection, namely SHARPPUNT, an in-memory dropper, and BACKPUNT, an embedded payload written in C#. Managed Defense also observed UNC2295 disable security tools to prevent identification and eradication efforts. The Managed Defense rapid response team worked to limit the impact of the breach and helped the organization quickly resume normal business operations.

Defensive Actions

Mandiant recommends the following steps to avoid attacks that use messaging platforms.

Perform regular phishing exercises

Perform regular phishing exercises against your user base, train and re-test users as needed.

Implement a Secure Email Gateway

Implement a Secure Email Gateway to analyze all inbound and outbound emails for malicious links and attachments.

Emails obtained from internal users should also be scanned and analyzed.

Block ports

Prevent users from installing unauthorized instant messaging applications.

Identify indicators of compromise in your environment

Disable the AlwaysInstallElevated privileges to ensure the current user's permission is required to install any Windows packages.

Trending Malware Families Observed

VIDAR
A data miner written in C++ which targets data from web browsers, cryptocurrency wallets, chat software, the Authy two-factor authentication utility and other applications.

QAKBOT
A backdoor written in C/C++ that implements a plug-in framework to extend its capabilities via embedded and downloaded plugins.

REDLINESTEALER
Malware capable of stealing credentials from web browsers, files, FTP applications and cryptocurrency wallets. It also collects extensive system survey information.

SQUIDGATE
A JavaScript-based backdoor commonly downloaded by SQUIDSLEEP. The malware collects basic system information and communicates via HTTP.

LYINGDOOR
A backdoor that is implemented as an MSBuild .NET inline task. It can execute commands, upload files from the system and download files to the system.

FLOOPYSTAMP
A simple reverse shell with no other functionality. The User-Agent and Host fields within its request header are selected randomly from a hardcoded list.

Related Resources

Pro-PRC “HaiEnergy” Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites

An AVADDON ransomware case study discussing how AVADDON, and various other Ransomware-as-a-Service services, prevailed in compromising critical targets with significant ransom demands.

Read More

The “Big Four”: Spotlight on China Podcast

An insider’s outlook on China’s cyber operations. Learn how they have transformed from “clumsy” to “stealthy” over time and how political and economic influences have shaped activities.

Listen Now

How to Detect and Stop a Ransomware Attack

Defenders need to be well-informed, practiced and swift. See what can happen in the short time a bad actor dwells in your network before it deploys ransomware and achieves its goal.

View the Timeline

Google Cloud

For more information visit cloud.google.com
MD-EXT-RT-EN-US-000425-03