SC Media
A CRA Resource

Threat Management, Threat Management

Newly identified APT group’s motives in Ukraine baffle researchers

Simon Hendery May 12, 2023

A view of a destroyed building after an industrial area was hit by a Russian missile in Kharkiv, Ukraine on June 29, 2022. Security researchers are baffled by the motives of Red Stinger, a group that has targeted victims on both sides of Russia’s war on Ukraine and even infected its own machines. (Photo by Sofia Bobok/Anadolu Agency via Getty Images)

Several advanced persistent threat attacks carried out across Ukraine between 2020 and 2022 have been linked to the same group of actors: a mystery entity whose allegiances are unclear.

Malwarebytes' research found Red Stinger/Bad Magic's attacks stretched back to 2020, and occurred in centers other than just Donetsk, Lugansk, and Crimea (which was annexed by Russia in 2014).

"Military, transportation and critical infrastructure were some of the entities being targeted, as well as some involved in the September [2022] East Ukraine referendums," the post said.

"Depending on the campaign, attackers managed to exfiltrate snapshots, USB drives, keyboard strokes, and microphone recordings."

The researchers said because of the contrasting nature of the attacks they have linked to the group, they couldn't attribute Red Stinger to a specific country.

"Any of the involved countries [in the Russia/Ukraine war] or aligned groups could be responsible, as some victims were aligned with Russia, and others were aligned with Ukraine," the blog stated.

An example of the baffling diversity of the targets of Red Stinger's attacks occurred gathering. The attackers used different layers of protection, had an extensive toolset for their victims, and the attack was clearly targeted at specific entities," the researchers wrote.

"Perhaps in the future, further events or additional activity from the group can shed light on the matter."

The researchers also uncovered evidence that, at some point, Red Stinger had infected its own machines. It was unclear whether that had been done by mistake or to carry out testing, they said, although the group's use of the names TstSCR and TstVM to identify two of its victims possibly suggested the action was a test.

Red Stinger's attack chain involves using malicious installer files to activate DBoxShell—malware that utilizes cloud storage services as a command-and-control mechanism—onto compromised Windows machines.

A Microsoft Software Installer (MSI) file is downloaded through a Windows shortcut file contained within a ZIP archive.

"This stage serves as an entry point for the attackers, enabling them to assess whether the targets are interesting or not, meaning that in this phase they will use different tools," the researchers said.

In the exfiltration phase of its operations, Red Stinger has used custom tools to steal data which may include a combination of screenshots, content from USB drives, keystroke logs and microphone recordings. The exfiltration phase of Red Stinger's attacks has been known to last up to several months.

marketing, he is a passionate storyteller who loves researching and sharing the latest industry developments.

Related

GENERATIVE AI

Report sheds light on global cybersecurity outlook

SC Staff January 17, 2024

Ongoing geopolitical instability has been noted by 70% of cybersecurity leaders around the world to be a key factor in their organizations' cybersecurity strategy, while nearly 50% said that cybersecurity will be dominated by generative artificial intelligence within the next two years, according to VentureBeat.

VULNERABILITY MANAGEMENT

Cyberattacks likely with PAX payment terminal bugs

SC Staff January 17, 2024

SecurityWeek reports that six vulnerabilities impacting PAX Technology's Android-based point-of-sale terminals that have already been addressed by the China-based payment terminal manufacturer could be leveraged to facilitate further compromise.

NETWORK SECURITY

Botnet fuels Androxgh0st malware’s punch

Simon Hendery January 17, 2024

“This particular attack is using unpatched vulnerabilities first announced (and patched) three to seven years ago. They are still unpatched and still being exploited,” researchers said.

Related Events

CYBERCAST

Real-world Insights from a Sophos Threat Analyst: It’s Great You Have a Firewall, But Here’s Why You Shouldn’t Skip Over MDR

On-Demand Event

CYBERCAST

Revolutionizing the essentials: Friction-minimizing approaches to overcoming advanced account takeover (ATO)

On-Demand Event

CYBERCAST

Evening the Odds Against Overpowered Cyber Adversaries: A Business Impact