THE GOOD
THE BAD
AND THE UGLY
IN CYBERSECURITY

The Good, the Bad and the Ugly in Cybersecurity – Week 11

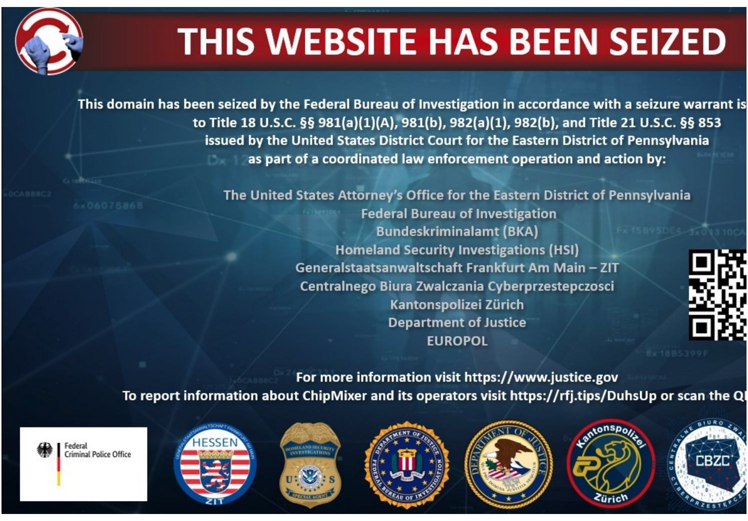
March 17, 2023
by SentinelOne

The Good

Good news this week as "one of the darkweb's largest cryptocurrency laundromats", unlicensed crypto platform ChipMixer, was seized and shutter
U.S., Swiss, Polish and German law enforcement agencies.

ChipMixer, which began operating in 2017, specialized in obfuscating blockchain transactions to hide the trail of virtual currency assets. Known as '
sites attempt to disguise the true source and destinations of exchanges by breaking down and mixing cryptocurrency tokens from different transact

It is alleged that the service had been used to launder over $3 billion in Bitcoin, with a large percentage of that being proceeds of ransomware payn
marketplace payments and nation-state criminal activity. Notorious North Korean threat actor and cryptocurrency thief Lazarus is believed to have
with Russia's General Staff Main Intelligence Directorate (GRU), *aka* APT28, which is said to have used ChipMixer to hide purchases of hacking infra


THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant is
to Title 18 U.S.C. §§ 981(a)(1)(A), 981(b), 982(a)(1), 982(b), and Title 21 U.S.C. §§ 853
issued by the United States District Court for the Eastern District of Pennsylvania
as part of a coordinated law enforcement operation and action by:

The United States Attorney's Office for the Eastern District of Pennsylvania
Federal Bureau of Investigation
Bundeskriminalamt (BKA)
Homeland Security Investigations (HSI)
Generalstaatsanwaltschaft Frankfurt Am Main – ZIT
Centralnego Biura Zwalczania Cyberprzestepczosci
Kantonspolizei Zürich
Department of Justice
EUROPOL

For more information visit https://www.justice.gov
To report information about ChipMixer and its operators visit https://rfj.tips/DuhsUp or scan the Q

Authorities have seized the ChipMixer domain

Along with seizing the site, authorities also bagged around $46 million worth of cryptocurrency and charged a 49-year old Vietnamese national, Mir
operating an unlicensed money transmitting business, money laundering and identity theft.

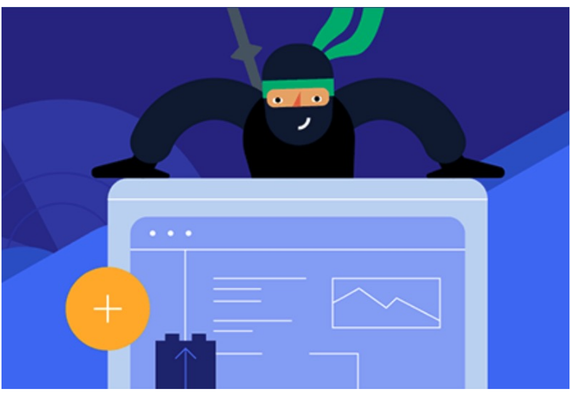
Nguyen, whose whereabouts remain unknown, openly flouted financial regulations. The DoJ's indictment says that he publicly derided efforts to cu
registered domain names and hosting services using stolen identities, pseudonyms and anonymous email services. If caught and convicted, Nguye

ChipMixer joins BestMixer, BitcoinFog and Helix in being shut down by U.S. and European law enforcement agencies for money laundering via crypt

The Bad

It was revealed this week that a U.S. Federal Agency had been breached by multiple threat actors, including a nation-state APT, through a software
since 2019. The breaches may have begun as early as August 2021 and occurred as late as November 2022.

According to an advisory from CISA published on Wednesday, threat actors exploited CVE-2019-18935, a .NET deserialization vulnerability in Prog
located in the agency's Microsoft IIS (Internet Information Services) web server to gain remote code execution.



Source: Telerik

CISA says it observed threat actors including known cybercrime gang XE Group uploading malicious DLLs, some disguised as PNG image files to the
These were then executed via the legitimate `w3wp.exe` process running on the compromised IIS servers. The attackers appear to have used timest
tactics, which involves changing the creation and modified dates on files to disguise their origin.

Much of the malware opened up reverse shells and allowed attackers interactive access to the compromised devices. ASPX webshells were also de
send, receive and delete files, and execute commands.

Interestingly, the Federal agency concerned had deployed an appropriate plugin to scan for the CVE-2019-18935 vulnerability but failed to detect
due to the Telerik UI software being installed in a file path that the scanner does not typically scan, a situation that may be common in other organi
installed software can vary depending on the organization and installation method.

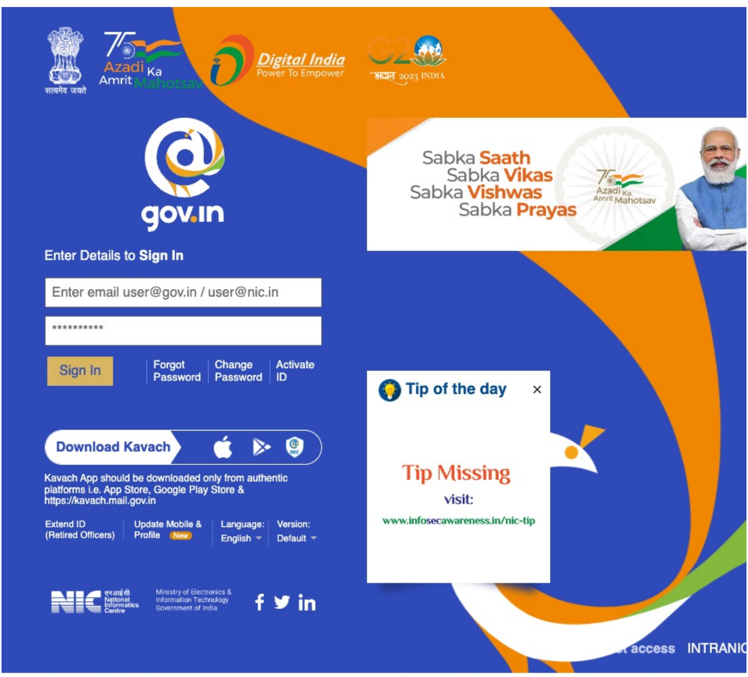
Organizations are advised to implement patch management solutions to ensure compliance with the latest security patches, and to update any inst
AJAX to the latest version. Security teams should review the detection and mitigations provided in the advisory for further information.

The Ugly

A threat actor group with interests closely aligned to those of the Russian and Belarussian governments was revealed to have been conducting a wi
espionage campaigns against Western governments and institutions this week by SentinelLabs researchers.

Winter Vivern, *aka* UAC-0114, was first spotted back in 2021 but appeared to have gone dark soon after. New activity was observed by the Polish C
end of January this year, but research published this week revealed a much wider set of campaigns that have targeted the Vatican, Indian governm
Ministry of Foreign Affairs as well as Polish and Ukrainian government agencies, among others. The campaigns have been ongoing through 2021 an
remained unreported until now.

Some of the group's latest tactics involve mimicking government domains, including government email login pages, to phish credentials and distrib



Enter Details to **Sign In**

Enter email user@gov.in / user@nic.in

****

Kavach App should be downloaded only from authentic platforms i.e. App Store, Google Play Store & https://kavach.mail.gov.in

Language: English
Version: Default

NIC National Informatics Centre
Ministry of Electronics & Information Technology Government of India
Sabka Saath
Sabka Vikas
Sabka Vishwas
Sabka Prayas
Azadi Ka Amrit Mahotsav

Tip of the day ×

Tip Missing
visit:
www.infosecawareness.in/nic-tip

E-GREETING
National Knowledge Network
Connecting Knowledge Institutions
eSampark
GeM NOMINATED FOR
GLOBAL WSIS 2
BE A PROUD I
VOTE FO

Although the group is not thought to be particularly technical, the researchers say that Winter Vivern makes creative use of simple batch scripts usi incidents, the threat actors utilized batch scripts disguised as virus scanners to download malware in the background while victims believed they w

The group also exploits application vulnerabilities to compromise specific targets. The SentinelLabs post says that in one incident, a malicious serv Acunetix web application vulnerability scanner, which may have served as a supplementary resource to scan target networks and possibly compro

More information about the Winter Vivern APT including indicators of compromise can be found in the SentinelLabs report here.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- The Good, the Bad and the Ugly in Cybersecurity – Week 12
- SentinelOne's Cybersecurity Predictions 2023 | What's Next?
- Apple's macOS Ventura | 7 New Security Changes to Be Aware Of
- Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
- Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool

©2023 SentinelOne. All Rights Reserved.