TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

February 2021

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

'WORLD'S MOST DANGEROUS MALWARE' EMOTET SHUT DOWN BY EUROPOL

Emotet has been one of the most destructive malwares of recent years. Initially, Emotet was a banking Trojan thought to have originated in Russia that was deployed against various financial institutions. Around 2016 and 2017, Emotet authors morphed the malware's function to make it a payload downloader and distributed it via macros (especially Word documents).

Essentially, Emotet acted as a loader for other malicious code on an infected host. The malware was usually distributed via botnets and was employing parked domains to distribute the malware. What made it so dangerous was how widely it was distributed among criminal organizations. The damage was significant, and it made cybersecurity professionals incredibly concerned.

Continued on next page...

But Emotet may finally be a thing of the past according to a Europol press release. The release states that a multifaceted criminal justice operation was undertaken by the following nation-states and organizations: The Netherlands (Europol's headquarters), Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine, "with international activity coordinated by Europol and Eurojust." Europol used the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) to execute the operation and take down what it called the "world's most dangerous malware."

The exact details of how Emotet was effectively shut down can be found in the following excerpt from the press release:

"The infrastructure that was used by EMOTET involved several hundreds of servers located across the world, all of these having different functionalities in order to manage the computers of the infected victims, to spread to new ones, to serve other criminal groups, and to ultimately make the network more resilient against takedown attempts.

To severely disrupt the EMOTET infrastructure, law enforcement teamed up together to create an effective operational strategy. It resulted in this week's action whereby law enforcement and judicial authorities gained control of the infrastructure and took it down from the inside. The infected machines of victims have been redirected towards this law enforcement-controlled infrastructure. This is a unique and new approach to effectively disrupt the activities of the facilitators of cybercrime."

Multiple arrests have been made in connection with this operation, and as more information is released, we will update the story. Emotet may be a thing of the past, but don't drop your guard. When one malware operation dies, there is inevitably another to take its place.—*Derek Kortepeter for Techgenix*

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-TECH (option 2)

Sales@TechHero.com

Software bug causes deletion of thousands of UK arrest records

Reports from news sources in the United Kingdom are shining a light on a rather bizarre incident. Originally reported by The Times of London, a major software bug has allowed 15,000 personal records from arrests in the UK to be deleted from the British Police National Computer (PNC) system. Most notably this software bug, believed to be a mix of human error and bad code, has eliminated vital biometric data that British police rely on for impending investigations.

The damage from this incident appears to have widespread ramifications. As reported by The Guardian, this may cause over 400,000 current crime records to be compromised by the blunder. Political pressure is mounting on Home Secretary Priti Patel to get the situation under control. Many are calling for the Home Office to give a full, transparent account of how this deletion of thousands of UK arrest records could have taken place.

Continued on next page...

In a letter addressed to the National Police Chiefs' Council (NPCC), deputy chief constable Naveed Malik had this to say on the situation:

"*As the National DNA Database and the National Fingerprint Collection currently contain incomplete sets of biometric records, there is the possibility that biometric matches between crime scenes and offenders may not be identified... We are aware of a couple of instances of 'near misses' for serious crimes where a biometric match to an offender was not generated as expected but the offender was identified through matches between scenes. However, in these circumstances, without a direct match report to the subject, it may be more challenging for police to progress to an interview or arrest... We are also aware of at least one instance where the DNA profile from a suspect in custody did not generate a match to a crime scene as expected, potentially impeding the investigation of the individual's involvement in the crime.*"

The Home Office has not been radio silent on the issue, however, as the highly publicized nature of this case has forced a response. The Home Office has told various U.K. media that they are currently working with British police to determine how much damage has been done. As far as they can find in their preliminary investigation, the Home Office believes that the deletion occurred as a result of a weekly clutter reduction in the database. The BBC, meanwhile, reported that the Home Office said that "no records of criminal or dangerous persons had been deleted."—*Derek Kortepeter for Techgenix*

Client Spotlight

The Epilepsy Association (formerly The Epilepsy Association of Central Florida) is dedicated to improving the quality of life for persons affected by epilepsy and seizure disorders. Not only does The Epilepsy Association provide related medical and case management services for those with epilepsy but we also offer educational programs to understand epilepsy for your business, community group, school, etc.

In addition, The Epilepsy Association reaches millions more every month through an award-winning epilepsy education news and information site. EpilepsyU.com is used by over 4,000,000 people in over 150 countries.

SOLARWINDS INVESTIGATION UNCOVERS NEW RAINDROP MALWARE

A series of malware strains have come out of the woodwork since the SolarWinds security incident. The newest malware, called Raindrop, is the fourth strain to emerge following its predecessors and researchers are releasing data on its mechanisms. Raindrop seems to build on its predecessors (Teardrop, Sunspot, and Sunburst) in numerous ways, though researchers are finding the greatest similarities with Teardrop. Researchers at Symantec describe Raindrop as “an additional piece of malware used in the SolarWinds attacks.”

Continued on next page...

Symantec released a thorough investigative piece on Raindrop. The primary function of the malware is much like Teardrop in that it acts as a backdoor deliverer of Cobalt Strike. While Cobalt Strike was created as a white hat penetration testing tool, it also has a history of being used by cybercriminals to create command and control (C2) servers. Unlike Teardrop, which is injected via the Sunburst backdoor, Raindrop has not been shown to have any direct connection to Sunburst.

Symantec says the following about Raindrop's activity:

"*Raindrop is compiled as a DLL, which is built from a modified version of 7-Zip source code. The 7-Zip code is not utilized and is designed to hide malicious functionality added by the attackers...*

Whenever the DLL is loaded, it starts a new thread from the DllMain subroutine that executes the malicious code. This malicious thread performs the following actions:"

- Executes some computation to delay execution. This does not affect functionality.
- Locates start of the encoded payload which is embedded within legitimate 7-Zip machine code.

"*In order to locate the start of the encoded payload, the packer uses stenography by scanning the bytes starting from the beginning of the subroutine and skipping any bytes until the first occurrence of the following bytes that represent operation codes (opcodes) of interest:*

.data:0000000180053008 opcodes db 5, 0Dh, 15h, 1Dh, 25h, 2Dh, 35h, 3Dh, 0B8h"

Following all of this, the payload is decrypted and decompressed. The encryption used by the payload is AES and for compression, it uses the LMZA algorithm. The main goal of Raindrop is to spread throughout a target's network, and based on its construction, it is incredibly capable of doing this.

—*Derek Kortepeter for Techgenix*