March 2022's Most Wanted Malware: Easter Phishing Scams Help Emotet Assert its Dominance

checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/

San Carlos, CA — Tue, 12 Apr 2022
Check Point Research (CPR), the Threat Intelligence arm of Check Point® Software Technologies Ltd. (NASDAQ: CHKP), a leading provider of cyber security solutions globally has published its latest Global Threat Index for March 2022. Researchers report that Emotet is continuing its reign as the most popular malware, impacting 10% of organizations worldwide, double that of February.

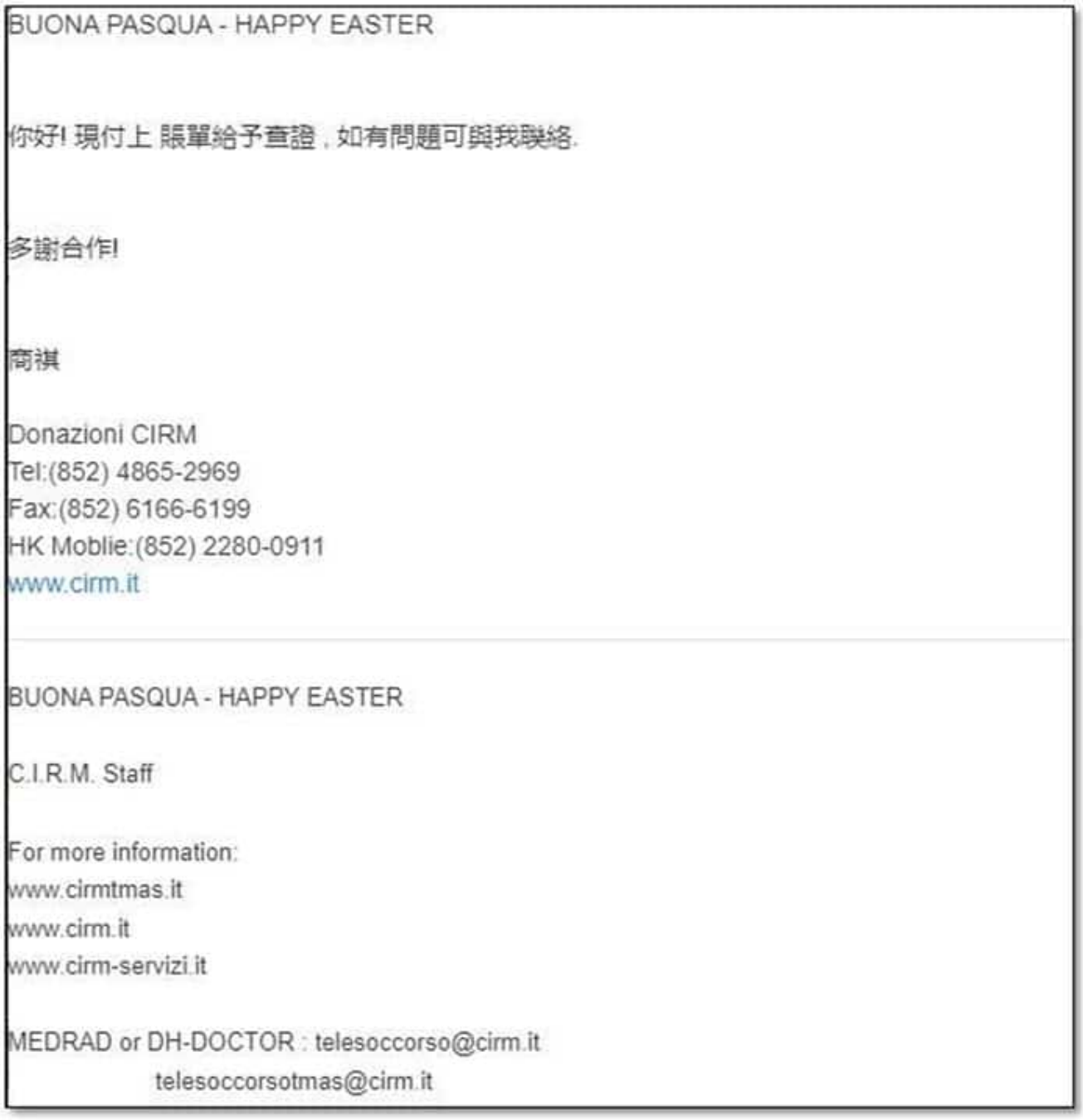
Emotet is an advanced, self-propagating and modular trojan that uses multiple methods for maintaining persistence and evasion techniques to avoid detection. Since its return in November last year and the recent news that Trickbot has shut down, Emotet has been strengthening its position as the most prevalent malware. This was solidified even further this month as many aggressive email campaigns have been distributing the botnet, including various Easter-themed phishing scams exploiting the buzz of the festivities. These emails were sent to victims all over the world with one such example using the subject "Buona Pasqua, happy easter" yet attached to the email was a malicious XLS file to deliver Emotet.

This month, Agent Tesla, the advanced RAT functioning as a keylogger and information stealer, is the second most prevalent malware, after appearing fourth in last month's index. Agent Tesla's rise is due to several new mal-spam campaigns delivering the RAT via malicious xlsx/pdf files worldwide. Some of these campaigns have leveraged the Russia/Ukraine war to lure victims.

"Technology has advanced in recent years to such a point where cybercriminals are increasingly having to rely on human trust in order to get through to a corporate network. By theming their phishing emails around seasonal holidays such as Easter, they are able to exploit the buzz of the festivities and lure victims into downloading malicious attachments that contain malware such as Emotet. In the run up to the Easter weekend, we expect to see more of these scams and urge users to pay close attention, even if the email looks like it's from a reputable source. Easter isn't the only public holiday and cybercriminals will continue to deploy the same tactics to inflict harm," said Maya Horowitz, VP of Research at Check Point Software. "This month we also observed Apache Log4j becoming the number one most exploited vulnerability again. Even after all the talk about this vulnerability at the end of last year, it is still causing harm months after the initial detection. Organizations need to take immediate action to prevent attacks from happening."

CPR also revealed this month that Education/Research is still the number one most attacked industry globally, followed by Government/Military and Internet Service Providers/Managed Service Providers (ISP/MSP). “Web Server Exposed Git Repository Information Disclosure” is now the second most commonly exploited vulnerability, impacting 26% of organizations worldwide, while “Apache Log4j Remote Code Execution” takes the top spot, impacting 33% of organizations. “HTTP Headers Remote Code Execution (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-13756)” keeps hold of third place with a global impact of 26%.

Examples of Easter-themed phishing emails


BUONA PASQUA - HAPPY EASTER

你好! 現付上 賬單給予查證 , 如有問題可與我聯絡.

多謝合作!

商祺

Donazioni CIRM
Tel:(852) 4865-2969
Fax:(852) 6166-6199
HK Moblie:(852) 2280-0911
www.cirm.it

BUONA PASQUA - HAPPY EASTER

C.I.R.M. Staff

For more information:
www.cirmtmas.it
www.cirm.it
www.cirm-servizi.it

MEDRAD or DH-DOCTOR : telesoccorso@cirm.it
telesoccorsotmas@cirm.it

Figure 1 Example of Easter Phishing Email

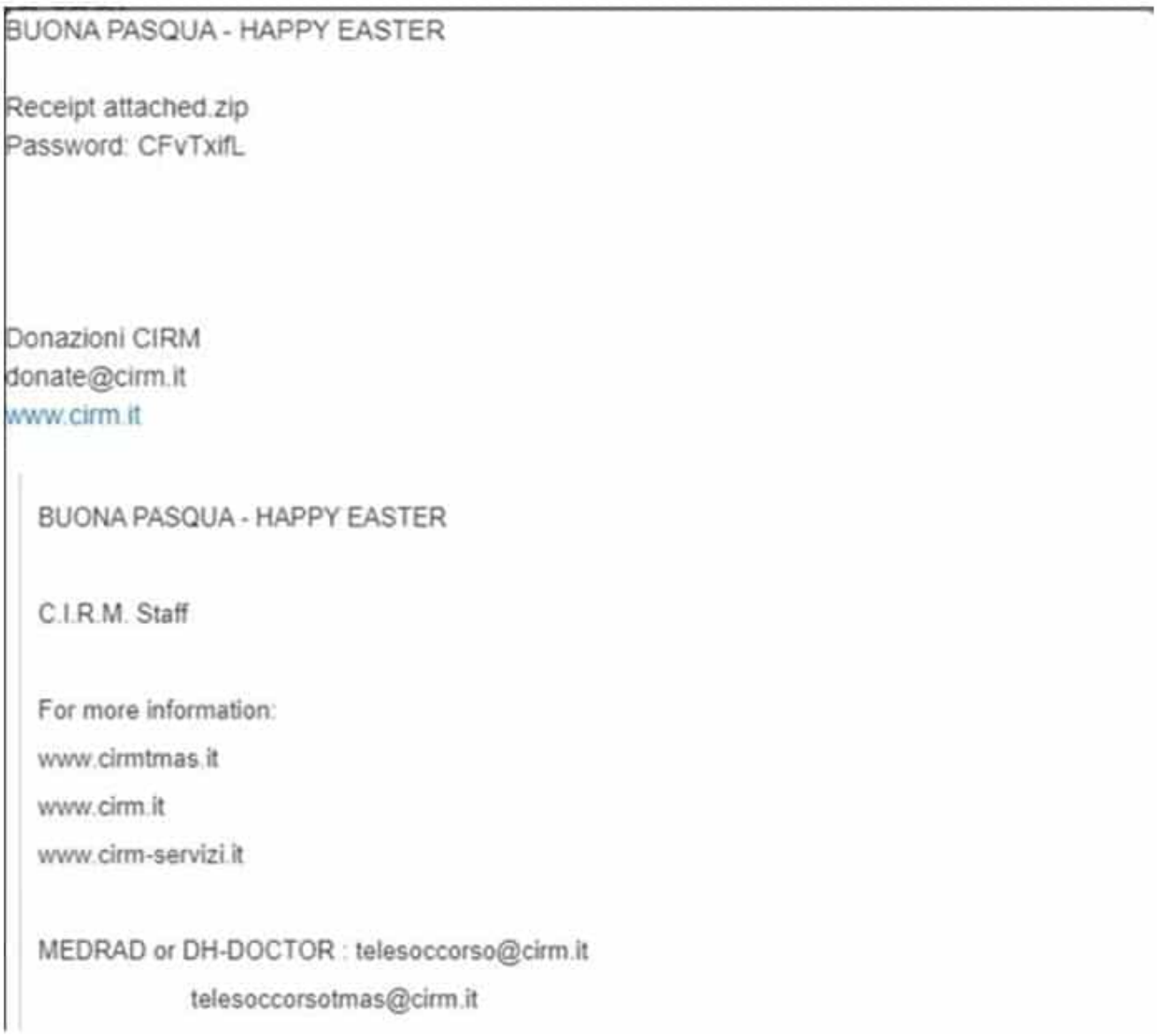


Figure 2 Example of an Easter Phishing Email sent to various countries

Top Malware Families
**The arrows relate to the change in rank compared to the previous month.*

This month, Emotet is still the most popular malware with a global impact of 10% of organizations worldwide, followed by Agent Tesla and XMRig both impacting 2% of organizations each.

1. ↔ **Emotet** – Emotet is an advanced, self-propagate, and modular Trojan. Emotet was once used to employ as a banking Trojan, and recently is used as a distributor to other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, it can be spread through phishing spam emails containing malicious attachments or links.

2. ↑ **Agent Tesla** – Agent Tesla is an advanced RAT functioning as a keylogger and information stealer, which is capable of monitoring and collecting the victim's keyboard input, system keyboard, taking screenshots, and exfiltrating credentials to a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and the Microsoft Outlook email client).
3. ↑ **XMRig** – XMRig is an open-source CPU mining software used for the mining process of the Monero cryptocurrency and was first seen in-the-wild May 2017.

Top Attacked Industries Globally
This month Education/Research is the number one most attacked industry globally, followed by **Government/Military** and **ISP/MSP**.

1. Education/Research
2. Government/Military
3. ISP/MSP

Top Exploited Vulnerabilities
This month "**Apache Log4j Remote Code Execution**" is the most commonly exploited vulnerability, impacting 33% of organizations globally, followed by "**Web Server Exposed Git Repository Information Disclosure**" which dropped from first place to second place and impacts 26% of organizations worldwide. "**HTTP Headers Remote Code Execution**" is still in third place in the top exploited vulnerabilities list, with a global impact of 26%.

1. ↑ **Apache Log4j Remote Code Execution (CVE-2021-44228)** – A remote code execution vulnerability exists in Apache Log4j. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the affected system.
2. ↓ **Web Server Exposed Git Repository Information Disclosure** – An information disclosure vulnerability has been reported in Git Repository. Successful exploitation of this vulnerability could allow an unintentional disclosure of account information.
3. ↔ **HTTP Headers Remote Code Execution (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756)** – HTTP headers let the client and the server pass additional information with an HTTP request. A remote attacker may use a vulnerable HTTP Header to run arbitrary code on the victim machine.

Top Mobile Malware
This month AlienBot is the most prevalent mobile malware, followed by xHelper and FluBot.

1. **AlienBot** – AlienBot malware family is a Malware-as-a-Service (MaaS) for Android devices that allows a remote attacker, at a first step, to inject malicious code into legitimate financial applications. The attacker obtains access to victims' accounts, and eventually completely controls their device.

2. **xHelper** – A malicious application seen in the wild since March 2019, used for downloading other malicious apps and display advertisement. The application is capable of hiding itself from the user and reinstalling itself if uninstalled.
3. **FluBot**– FluBot is an Android malware distributed via phishing SMS messages (Smishing), most often impersonating logistics delivery brands. Once the user clicks the link inside the message, they are redirected to the download of a fake application containing FluBot. Once installed the malware has various capabilities to harvest credentials and support the Smishing operation itself, including uploading contact lists, as well as sending SMS messages to other phone numbers.

Check Point's Global Threat Impact Index and its ThreatCloud Map is powered by Check Point's ThreatCloud intelligence. ThreatCloud provides real-time threat intelligence derived from hundreds of millions of sensors worldwide, over networks, endpoints and mobiles. The intelligence is enriched with AI-based engines and exclusive research data from Check Point Research, The Intelligence & Research Arm of Check Point Software Technologies.

The complete list of the top 10 malware families in February can be found on the Check Point blog.

Follow Check Point Research via:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

About Check Point Research
Check Point Research (CPR) provides leading cyber threat intelligence to Check Point Software customers and the greater intelligence community. The research team collects and analyzes global cyber-attack data stored on ThreatCloud to keep hackers at bay, while ensuring all Check Point solutions are updated with the latest protections. The research team consists of over 100 analysts and researchers cooperating with other security vendors, law enforcement and various CERTs.