Cyber Directorate
Department of the Army
Criminal Investigation Division

Cybercrime Prevention Flyer

CPF 0050-22-CID461-9H **16 November 2022**

Malware-as-a-Service: Raccoon Infostealer

Malware-as-a-Service (Maas) is the paid use, a rental, of malicious software for the purposes of executing cyber attacks. One such MaaS responsible for a worldwide cybercrime spree was the Raccoon Infostealer.

Infecting computers from 2018 to early 2022, the Raccoon Infostealer, enabled cybercriminals to steal millions of unique credentials and other forms of identification such as email addresses, bank account information, cryptocurrency addresses, credit card numbers, etc., from millions of victims. Included in the stolen data, are more than 4 million email addresses.

In March of 2022, Dutch authorities arrested the Raccoon Infostealer principal developer, Ukrainian national Mark Sokolovsky. Sokolovsky, fleeing mandatory Ukrainian military service following the recent Russian invasion, made an operational security flaw by connecting a personal account to Raccoon Infostealer. He also left the Ukraine with a companion who documented their travel to the Netherlands via social media.

Under investigation by international law enforcement and an FBI Cyber Task Force, which included Department of the Army CID, the Raccoon Infostealer server was taken down and Sokolovsky is pending extradition to the U.S.

Due to the enormity of Raccoon Infostealer compromises, the FBI established a Raccoon Infostealer Disclosure portal for individuals to determine if their email address was captured by Raccoon Infostealer.

Report a crime to the Department of the Army Criminal Investigation Division

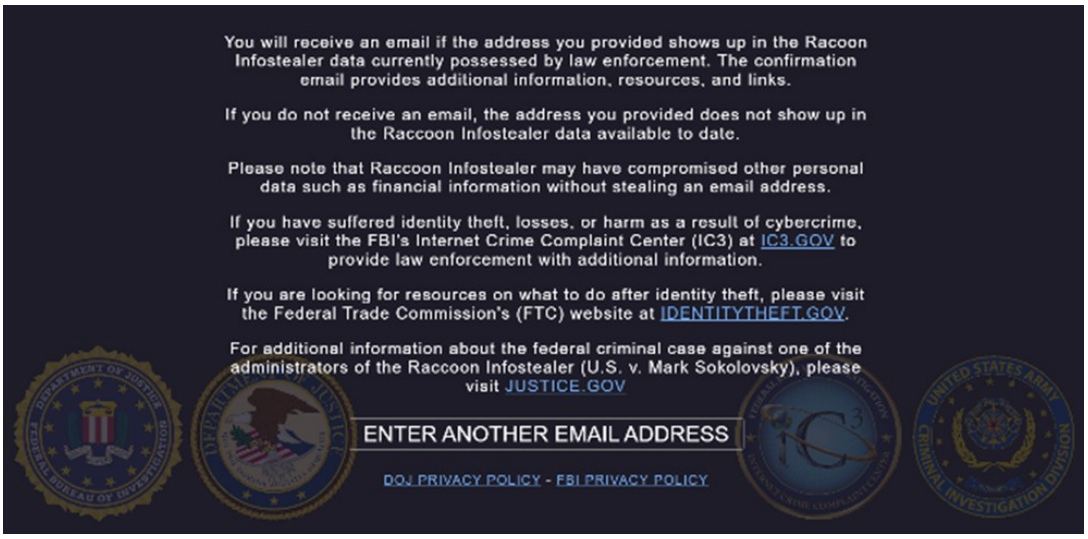
Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

When an email address is submitted, the following response will appear.



Only one email address may be submitted at a time. However, there is no cap on how many email addresses an individual can query.

Victims of Raccoon Infostealer or another data compromise should always submit a complaint to the FBI's Internet Crime Complaint Center (IC3).

Additional Resources:

United States Department of Justice - Newly Unsealed Indictment Charges Ukrainian National with International Cybercrime Operation

New Jersey Cybersecurity and Communications Integration Cell – Raccoon Threat Profile

Antivirus Home Use Program – No Cost for DoD Employees

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF