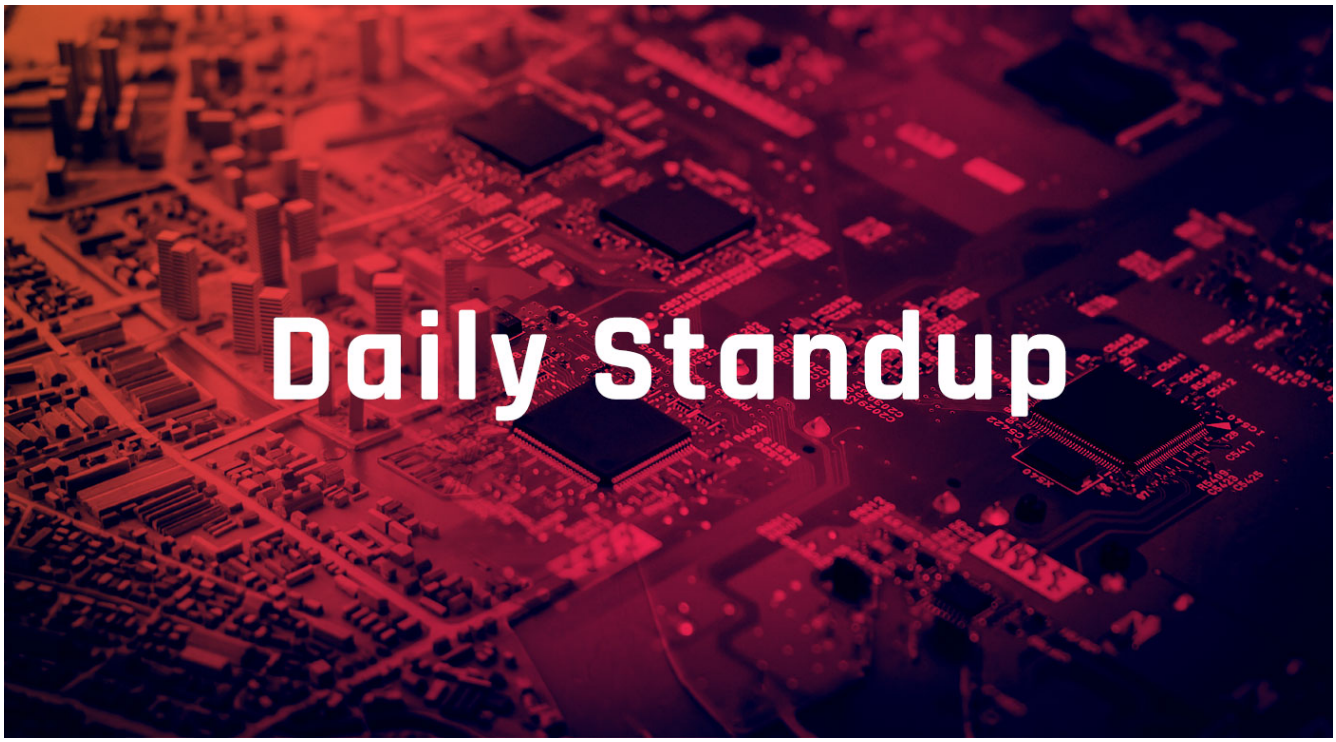
FLASHPOINT

Intelligence Report

Daily Standup

August 21, 2023



Interpol Arrests 14 Who Allegedly Scammed $40m from Victims in 'Cyber Surge' (Register)

Target audience: Authentication Teams, Fraud Teams, Security Ops, Threat Intel/CTI

Summary: *An Interpol-led operation arrested 14 suspects and identified 20,674 "suspicious" networks spanning 25 African countries that international cops have linked to more than $40 million in cybercrime losses. Africa Cyber Surge II, a combined police operation which began in April and lasted four months, was a coordinated effort between Interpol, African law enforcement, and private-sector security firms to disrupt online extortion, phishing, business email compromise (BEC) and other cyber scams. But given that BEC scams cost billions of dollars a year it's small change. Interpol, Afripol, and infosec companies Group-IB and Uppsala Security provided on-the-ground operational support, the international agency said. This included helping with three arrests in Cameroon related to an online scam involving the fraudulent sale of works of art worth $850,000. Additionally, police in Nigeria arrested a suspect who allegedly defrauded a victim in Gambia, and police in Mauritius arrested two suspected money mules linked to messaging platform scams. Plus, Cameroonian authorities took down two darknet sites, and Kenyan law enforcement shut down 615 malware separate hosting operations.*

Analyst comment: This joint endeavor between African law enforcement, private-sector security firms, and Interpol aimed to curb several cyber threats, including business email compromise, phishing, and online extortion. Despite its achievements, the scope of this crackdown is relatively minor compared to the billions lost annually to BEC scams. The growing concern over cybercrime in Africa demonstrates the importance of international cooperation to combat these threats.

See also:

"Cybercrime: 14 Arrests, Thousands of Illicit Cyber Networks Disrupted in Africa Operation" (Interpol)

"Business Email Compromise Threat Landscape" (Flashpoint)

Suspected N. Korean Hackers Target S. Korea-US Drills (SecurityWeek)

Target audience: CISO, CIO, Security Engineers, Security Ops, Threat Intel/CTI

Summary: *Suspected North Korean hackers have attempted an attack targeting a major joint military exercise between Seoul and Washington that starts on Monday, South Korean police said. South Korea and the United States will kick off the annual Ulchi Freedom Shield drills on Monday through August 31 to counter growing threats from the nuclear-armed North. Pyongyang views such exercises as rehearsals for an invasion and has repeatedly warned it would take "overwhelming" action in response. The hackers — believed to be linked to a North Korean group dubbed Kimsuky — carried out "continuous malicious email attacks" on South Korean contractors working at the allies' combined exercise war simulation centre, the Gyeonggi Nambu Provincial Police Agency said in a statement on Sunday. A joint investigation by the police and the US military found that the IP address used in the latest attack matched one identified in a 2014 hack against South Korea's nuclear reactor operator blamed on the group, according to the statement.*

Analyst comment: The hacking group believed to be Kimsuky is said to have targeted South Korean contractors involved in war simulation exercises using "spearphishing" techniques. South Korean police stated that no military-related information was compromised. Investigations revealed similarities between this cyberattack and a 2014 hack against South Korea's nuclear reactor operator. Kimsuky's primary objectives reportedly include gathering intelligence on foreign policy and national security topics related to the Korean peninsula.

See also:

"The Republic of Korea and United States Announce Exercise Ulchi Freedom Shield 23" (US Navy)

Key Developments: Asia-Pacific (Flashpoint)

This Malware Turned Thousands of Hacked Windows and MacOS PCs into Proxy Servers (Hacker News)

Target audience: CISO, CIO, Security Engineers, Security Ops, Threat Intel/CTI, Windows or Unix Admin Teams

Summary: *Threat actors are leveraging access to malware-infected Windows and macOS machines to deliver a proxy server application and use them as exit nodes to reroute proxy requests. According to AT&T Alien Labs, the unnamed company that offers the proxy service operates more than 400,000 proxy exit nodes, although it's not immediately clear how many of them were co-opted by malware installed on infected machines without user knowledge and interaction. Multiple malware families have been observed delivering the proxy to users searching for cracked software and games. The proxy software, written in the Go programming language, is capable of targeting both Windows and macOS, with the former capable of evading detection by using a valid digital signature. In addition to receiving further instructions from a remote server, the proxy is configured to gather information about the hacked systems, including running processes, CPU and memory utilization, and battery status. What's more, the installation of the proxy software is accompanied by the deployment of additional malware or adware elements. The disclosure builds upon prior findings from AT&T in which macOS machines compromised by AdLoad adware are being corralled into a giant, residential proxy botnet, raising the possibility that the operators of AdLoad could be running a pay-per-Install campaign.*

Analyst comment: Researchers have identified a concerning trend in which threat actors use malware to co-opt Windows and MacOS devices, allowing potentially malicious activity to be routed through these machines. The MacOS ecosystem, once considered relatively safer, has seen a significant uptick in targeting by cybercriminals, driven by its increased corporate use and the potential financial gains for threat actors. Analysts recommend users stay current with security patches and exercise caution with unsolicited software downloads.

See also:

"ProxyNation: The Dark Nexus between Proxy Apps and Malware" (AT&T)

Breaches and Malware (Flashpoint)

Additional stories are included below, as they are of interest to threat intelligence teams:

"Thousands of Android APKs Use Compression Trick to Thwart Analysis" (BleepingComputer)

"Cuba Ransomware Uses Veeam Exploit against Critical US Organizations" (BleepingComputer)

"Hackers Use VPN Provider's Code Certificate to Sign Malware" (BleepingComputer)

"Microsoft: BlackCat's Sphynx Ransomware Embeds Impacket, RemCom" (BleepingComputer)

"Hackers Ask $120,000 for Access to Multi-Billion Auction House" (BleepingComputer)

"How EU Lawmakers Can Make Mandatory Vulnerability Disclosure Responsible" (Help Net Security)

“Add 'Writing Malware' to the List of Things Generative AI Is Not Very Good at Doing” (Register)

“HiatusRAT Malware Resurfaces: Taiwan Firms and U.S. Military Under Attack” (Hacker News)

“Federally Insured Credit Unions Required to Report Cyber Incidents within 3 Days” (SecurityWeek)

“Stealthy ‘LabRat’ Campaign Abuses TryCloudflare to Hide Infrastructure” (SecurityWeek)

“Flaws in Juniper Switches and Firewalls Can Be Chained for Remote Code Execution” (SecurityWeek)

“US Gov Warns of Foreign Intelligence Cyberattacks against US Space Industry” (SecurityWeek)

Please find past standups at https://fp.tools/home/intelligence/standup.