Proprietary Software and Security Issues

By Roy Schestowitz
Created 09/11/2021 - 5:13pm

- **Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer** [3] [iophk: Windows TCO]

  Both Godzilla and NGLite were developed with Chinese instructions and are publicly available for download on GitHub. We believe threat actors deployed these tools in combination as a form of redundancy to maintain access to high-interest networks. Godzilla is a functionality-rich webshell that parses inbound HTTP POST requests, decrypts the data with a secret key, executes decrypted content to carry out additional functionality and returns the result via a HTTP response. This allows attackers to keep code likely to be flagged as malicious off the target system until they are ready to dynamically execute it.

- **[Crackers] breach nine global organizations in ongoing espionage campaign** [4] [iophk: Windows TCO]

  A [cracking] group with potential ties to China has breached nine global organizations as part of an ongoing espionage effort mostly targeting the defense sector, findings made public Sunday revealed.

  According to a report from cybersecurity company Palo Alto Networks, the [crackers] targeted at least 370 organizations running potentially vulnerable Zoho servers in the U.S. alone, successfully compromising at least one, as part of a wider global campaign.
Europol on Monday announced the arrests, which took place Thursday, saying that the two individuals arrested are alleged to be behind more than 5,000 cyberattacks and are accused of having gained more than half a million Euros in ransomware payments made by victims.

The arrests were the latest in a string of operations pursued by a coalition of international partners against REvil, with Europol saying Monday that three other individuals associated with REvil, along with two others associated with a linked cyber crime group, have been arrested since February.

**REvil Ransom Arrest, $6M Seizure, and $10M Reward**

The U.S. Department of Justice today announced the arrest of Ukrainian man accused of deploying ransomware on behalf of the REvil ransomware gang, a Russian-speaking cybercriminal collective that has extorted hundreds of millions from victim organizations. The DOJ also said it had seized $6.1 million in cryptocurrency sent to another REvil affiliate, and that the U.S. Department of State is now offering up to $10 million for the name or location any key REvil leaders, and up to $5 million for information on REvil affiliates.

**DOJ charges 2 men allegedly behind REvil ransomware attacks**

Yaroslav Vasinskyi, a Ukrainian national arrested last month in Poland, and Yevgeniy Polyanin, a Russian national who remains at large, face charges of fraud, conspiracy and money laundering. Vasinskyi was charged in connection with his alleged role in carrying out the devastating July 4 ransomware attack against the software firm Kaseya, which in turn affected hundreds of companies within the U.S.

**77% Indian organisations faced downtime due to cyber risk during festive season**

New Delhi, During peak festive season in the last 18 months 77 per cent of organisations in India experienced downtime due to cybersecurity risk, while 81 per cent of global organisations experienced increased cyber threats during Covid-19, a new report revealed on Tuesday.

According to McAfee Enterprise and FireEye's report titled 'Cybercrime in a Pandemic World: The Impact of Covid-19', the top three most threatening cyber risks that were detected are malware attacks (47 per cent), data breaches (43 per cent), ransomware and cloud jacking (33 per cent each), over 30 per cent of the IT professionals also experienced vulnerabilities in
their 'Internet of Things' devices.

- **SolarWinds investors sue company over supply chain attacks** [9][iophk: Windows TCO]

  The attacks came to light in December 2020 when American cyber security firm FireEye announced that it had identified a global campaign to compromise public and private sector bodies through corruption of software supply chains.

  FireEye is now known as Mandiant, taking on the name of a company that it acquired some years ago after selling its network, email and cloud security products, as well as the FireEye name, in June this year.

- **McAfee Corp to be taken private in $14-billion deal** [10]

  The investor group will acquire all outstanding shares of McAfee common stock for $26 per share in an all-cash deal that values McAfee at about $12 billion on an equity basis.

- **npm install is curl | bash** [11]

  npm (and yarn) will execute arbitrary code when you install a package via install scripts. A valid use-case is to build native code on installation, or do some other environment-specific setup, though these scripts have also been used to show ads and, of course, as an attack vector. In fact, install scripts were the most popular route for malware as of 20192.

  Installing a single malicious package is enough to get reasonably pwned. The risk is mitigated by npm?'s moderation of the registry ? they?re quick to remove malware once discovered. This works pretty well, though I worry about the day someone uses this to publish a self-replicating worm.

  This attack vector isn?t unique to npm. Other package managers like pip and RubyGems allow for the same thing. As developers, we?re not as cautious when installing packages from these registries as when we use curl | bash, though we should be3.

- **New DDoS attack vectors may spell trouble in future: Kaspersky** [12]

  Researchers at the Universities of Maryland and Colorado Boulder were credited with the TCP development, while the second was credited to security firm NexusGuard and named Black
Storm.

The TCP attack targets devices between a client and a server: firewalls, load balancers, network address translators, and deep packet inspection tools, many of which could interfere with a TCP connection.

Source URL: http://www.tuxmachines.org/node/157734

Links: