The last update by the CIS was on February 13, 2019. This indicate that the Security Alert level is remaining at Blue (Guarded)

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

08 March 2019

In The News This Week

Alphabet's Chronicle launched security telemetry service Backstory this week

Chronicle has debuted Backstory, a cloud-based cybersecurity telemetry service for the enterprise designed to give companies access to vast computing sources when examining their own security posture. Owned by Google's parent company Alphabet, Chronicle is a year-old cybersecurity company which originated from the X moonshot factory. Now established in its own right, the enterprise cybersecurity company says that its new product is "designed for a world that thinks in petabytes," and one that "will give enterprises a major leap over the current data storage and compute systems holding back their security." In a post on Medium.com this week, Chronicle documented how a year of releasing new features for VirusTotal -- which is also a part of the firm -- led to the challenge of finding the "backstory" which tied together malware, new threat alerts, internal network activity, and external attacks. As a result, Backstory has been developed. The global cloud service is described as a way for the enterprise to "privately upload, store, and analyse their internal security telemetry to detect and investigate potential cyber threats." The solution works by building a layer over Google infrastructure in which security telemetry data can be uploaded, including DNS traffic, endpoint logs, and proxy information. This data is then indexed and analysed, as well as compared against threat intelligence alerts and signals curated by Chronicle to detect potentially malicious activity. Chronicle says that the platform is also able to analyse historical data to notify administrators of any past access to malicious domains or malware-laden files which may indicate that a network is already at risk of compromise..
(Adapted from a ZDNet article found here: https://www.zdnet.com/article/alphabets-chronicle-launches-security-telemetry-service-backstory/)

NSA Releases GHIDRA 9.0 — Free, Powerful Reverse Engineering Tool

The United States' National Security Agency (NSA) today finally released GHIDRA version 9.0 for free, the agency's home-grown classified software reverse engineering tool that agency experts have been using internally for over a decade to hunt down security bugs in software and applications. GHIDRA is a Java-based reverse engineering framework that features a graphical user interface (GUI) and has been designed to run on a variety of platforms including Windows, macOS, and Linux. Reverse engineering a program or software involves disassembling, i.e. converting binary instructions into assembly code when its source code is unavailable, helping software engineers, especially malware analysts, understand the functionality of the code and actual design and implementation information. The existence of GHIDRA was first publicly revealed by WikiLeaks in CIA Vault 7 leaks, but the NSA today publicly released the tool for free at the RSA conference, making it a great alternative to expensive commercial reverse engineering tools like IDA-Pro. "It [GHIDRA] helps analyse malicious code and malware like viruses, and can give cybersecurity professionals a better understanding of potential vulnerabilities in their networks and systems," NSA official website says while describing GHIDRA. Speaking at RSA Conference, Senior NSA Adviser Robert Joyce assures GHIDRA contains no backdoor, saying "This is the last community you want to release something out to with a backdoor installed, to people who hunt for this stuff to tear apart." Joyce also said GHIDRA includes all the features expected in high-end commercial tools, with new and expanded functionality NSA uniquely developed, and supports a variety of processor instruction sets, executable format and can be run in both user-interactive and automated modes.
Read the full story on https://thehackernews.com/

Risks of File-Sharing Technology

What is file sharing?

File sharing involves using technology that allows internet users to share files that are housed on their individual computers. Peer-to-peer (P2P) applications, such as those used to share music files, are some of the most common forms of file-sharing technology. However, P2P applications introduce security risks that may put your information or your computer in jeopardy.

What risks does file-sharing technology introduce?

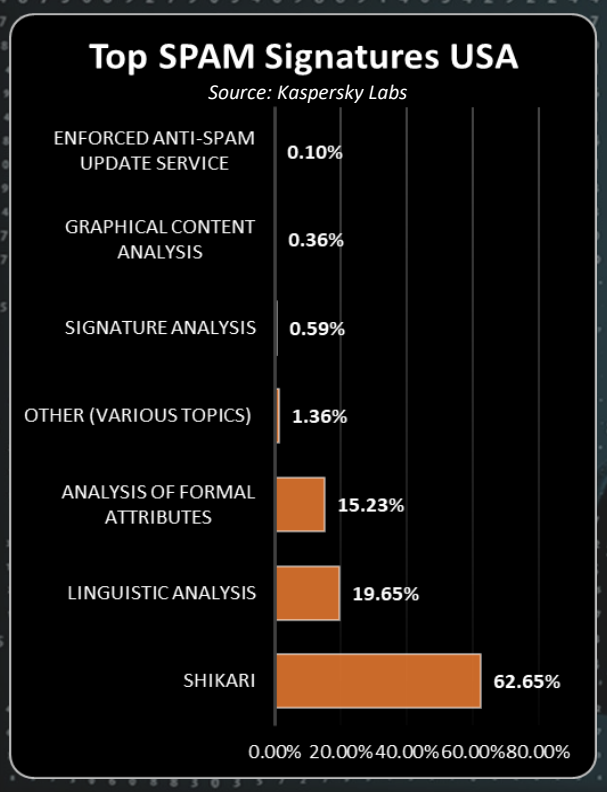
- Installation of malicious code - When you use P2P applications, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected (see Recognizing and Avoiding Spyware and Recovering from Viruses, Worms, and Trojan Horses for more information).
- Exposure of sensitive or personal information - By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft (see Protecting Your Privacy and Avoiding Social Engineering and Phishing Attacks for more information).
- Susceptibility to attack - Some P2P applications may ask you to open certain ports on your firewall to transmit the files. However, opening some of these ports may give attackers access to your computer or enable them to attack your computer by taking advantage of any vulnerabilities that may exist in the P2P application. There are some P2P applications that can modify and penetrate firewalls themselves, without your knowledge.
- Denial of service - Downloading files causes a significant amount of traffic over the network. This activity may reduce the availability of certain programs on your computer or may limit your access to the internet (see Understanding Denial-of-Service Attacks for more information).
- Prosecution - Files shared through P2P applications may include pirated software, copyrighted material, or pornography. If you download these, even unknowingly, you may be faced with fines or other legal action. If your computer is on a company network and exposes customer information, both you and your company may be liable.

How can you minimize these risks?

The best way to eliminate these risks is to avoid using P2P applications. However, if you choose to use this technology, you can follow some good security practices to minimize your risk:

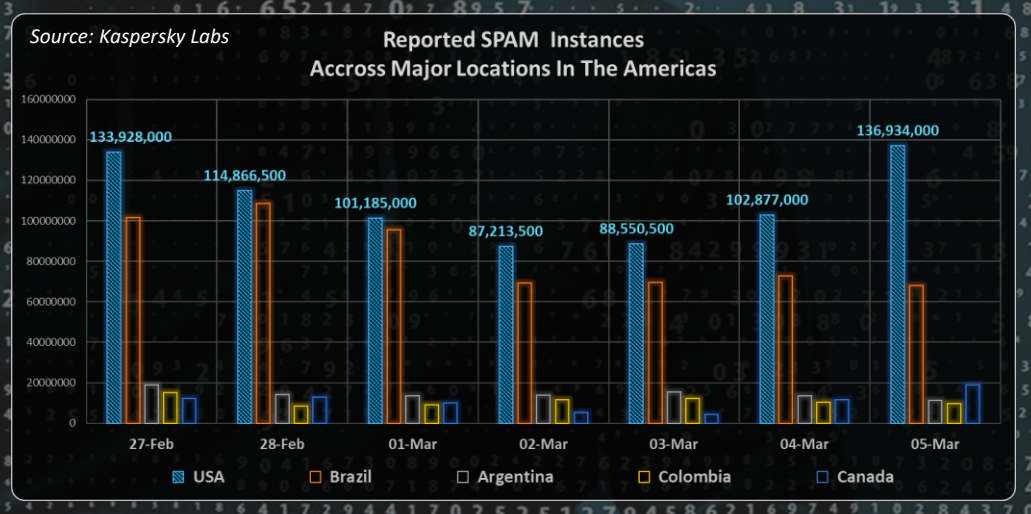
- use and maintain anti-virus software - Anti-virus software recognizes and protects your computer against most known viruses. However, attackers are continually writing new viruses, so it is important to keep your anti-virus software current (see Understanding Anti-Virus Software for more information).
- install or enable a firewall - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer (see Understanding Firewalls for more information). Some operating systems actually include a firewall, but you need to make sure it is enabled.

You can read the full story by Mindi McDowell, Brent Wrisley, and Will Dormann here:
https://www.us-cert.gov/ncas/tips/ST05-007



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

F-Secure posted on their Blog site that roughly **69%** of spam emails attempt to trick users into visiting a malicious URL. Malicious attachments were used in the remaining **31%** percent of spam.



Author: Chris Bester