Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On August 5, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in GRUB2, F5, Google and GNU products.

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

07 August 2020

In The News This Week

Confirmed: Garmin received decryptor for WastedLocker ransomware

BleepingComputer can confirm that Garmin has received the decryption key to recover their files encrypted in the WastedLocker Ransomware attack. On July 23rd, 2020, Garmin suffered a worldwide outage where customers could not access their connected services, including the Garmin Connect, flyGarmin, Strava, inReach solutions. BleepingComputer was the first to confirm that Garmin suffered a cyberattack by the WastedLocker Ransomware operators after employees shared photos of encrypted workstations, and we found a sample of the ransomware utilized in the attack. Employees later shared with BleepingComputer that the ransom demand was $10 million. After a four day outage, Garmin suddenly announced that they were starting to restore services, and it made us suspect that they paid the ransom to receive a decryptor. Garmin refused, though, to comment any further.
Read the full story here: BleepingComputer *(Thanks to my good friend Yazan Shapsugh who shared this news)*

U.S. Offers Reward of $10M for Info Leading to Discovery of Election Meddling

The U.S. government is concerned about foreign interference in the 2020 election, so much so that it will offer a reward of up to $10 million for anyone providing information that could lead to tracking down potential cybercriminals aiming to sabotage the November vote. The U.S. Department of State's Rewards for Justice (RFJ) program, overseen by the Diplomatic Security Service, will pay for info that can identify or locate someone working with or for a foreign government "for the purpose of interfering with U.S. elections through certain illegal cyber activities," according to a release posted on the department's website. The reward covers anyone seeking to interfere with an election at the federal, state or local level by violating or even aiding the violation of a U.S. law against computer fraud and abuse, according to the department.. Read the full article here: ThreatPost

Pen Testers Who Got Arrested Doing Their Jobs Tell All

Coalfire's Gary De Mercurio and Justin Wynn share the details of their physical penetration-testing engagement gone wrong, as well as recommendations for protecting all red teamers. When they first scanned the cardkey to the front entrance of the Dallas County Courthouse in Iowa, red-team experts Gary De Mercurio and Justin Wynn didn't hear the requisite click of a lock disengaging. It was after midnight on Sept. 11, 2019, the last leg of their penetration-testing engagement for the state of Iowa's Judicial Branch, and they got their first big surprise of that now-infamous evening. "Justin grabs the door and we look at each other, and I said, 'Did it work?' and he's like, 'No, it's open,'" recalls De Mercurio, a senior manager at Coalfire. "The door was locked, but they hadn't latched it all the way."
So the two social engineering and physical pen-test experts could get a more accurate take on the entrance security, Wynn closed the door and they started all over again with the cardkey, this time with the door locked. De Mercurio then slid a plastic cutting board retrofitted with a handy notch into the doorjamb and used it to unlatch the door. The pair figured they had somewhere between 20 to 30 seconds from then until the building alarm would sound, so they executed the usual next step in the physical testing process: checking the strength of the alarm's passcode settings by first typing in the system's default code as well as easy-to-guess combinations. Once the alarm sounded, the pair went back to work looking for other potential vulnerabilities in the courthouse while waiting to see if the authorities would respond. In three other facilities they had tested for the state agency, building alarms had not dialled out to law enforcement — a significant security hole. "I had my fingers crossed, hoping this one dials out and gives the client a softball win because everything else was pretty abysmal that we had encountered" security-wise, says Wynn, a senior security consultant at Coalfire. It did, and that's when the second big surprise came: an arrest, followed by felony charges, a night in the slammer, and nearly five months of a hellish legal quagmire driven mainly by a power struggle between state and county officials in Iowa over who had legal jurisdiction over the courthouse building they had entered.... Read the full story by Kelly Jackson Higgins here: Darkreading

Cybersecurity Red Team Versus Blue Team — Main Differences

Many of you have probably heard security experts talking about Red Team and Blue Team activities. Who are these teams, what do they do, and what is their purpose? I found a good article by SARA JELEN of SecurityTrails who explains it better than what I can. Below is a condensed version of the article, but I encourage you to visit the SecurityTrails site and read the full article.

When discussing cybersecurity, the terms "Red team" and "Blue team" are often mentioned. Long associated with the military, these terms are used to describe teams that use their skills to imitate the attack techniques that "enemies" might use, and other teams that use their skills to defend. In cybersecurity, there isn't much difference. With new regulations, including the enforcement of GDPR and their threats of financial penalties, organizations are rushing to empower their security infrastructures as they face the high risk of data breaches. Today we'll talk about Red team vs. Blue team, their importance, and why every company should utilize the abilities of these highly skilled professionals.
What is a "Red team"? - Red teams are focused on penetration testing of different systems and their levels of security programs. They are there to detect, prevent and eliminate vulnerabilities. A red team imitates real-world attacks that can hit a company or an organization, and they perform all the necessary steps that attackers would use. By assuming the role of an attacker, they show organizations what could be backdoors or exploitable vulnerabilities that pose a threat to their cybersecurity. A common practice is to hire someone outside the organization for red teaming — someone equipped with the knowledge to exploit security vulnerabilities, but unaware of the defences built into the organization's infrastructure. The techniques a red team uses vary from standard phishing attempts aimed at employees and social engineering to impersonating employees with the goal of obtaining admin access. To be truly effective, red teams need to know all the tactics, techniques and procedures an attacker would use.
Red teams offer critical benefits, including a better understanding of possible data exploitation and the prevention of future breaches. By simulating cyber attacks and network security threats, companies make sure their security is up to par with the proper defences in place.
What is a "Blue team"? - A blue team is similar to a red team in that it also assesses network security and identifies any possible vulnerabilities. But what makes a blue team different is that once a red team imitates an attacker and attacks with characteristic tactics and techniques, a blue team is there to find ways to defend, change and re-group defence mechanisms to make incident response much stronger. Like a red team, a blue team needs to be aware of the same malicious tactics, techniques and procedures in order to build response strategies around them. And blue team activity isn't exclusive to attacks. They're continuously involved to strengthen the entire digital security infrastructure, using software like an IDS (intrusion detection system) that provides them with an ongoing analysis of unusual and suspicious activity. Some of the steps a blue team incorporates are: ✦ Security audits, such as a DNS audit ✦ Log and memory analysis ✦ pcap (an API for capturing network traffic) ✦ Risk intelligence data analysis ✦ Digital footprint analysis ✦ Reverse engineering ✦ DDoS testing ✦ Developing risk scenarios.
Top 5 red team and blue team skills - The characteristics of red teams and blue teams are as different as the techniques they use. This will provide you more insight into the purpose and roles these two teams play. You'll also better understand if your own skills fit into these cybersecurity job descriptions, helping you choose the right road.
Red team skills (Get into the mind of an attacker and be as creative as they can be)

1. Think outside the box - The main characteristic of a red team is thinking outside the box; constantly finding new tools and techniques to better protect company security.
2. Deep knowledge of systems - Having deep knowledge of computer systems, protocols and libraries and known methodologies will give you a clearer road to success.
3. Software development - The benefits of knowing how to develop your own tools are substantial.
4. Penetration testing - Penetration testing is an essential part of red teams and is part of their "standard" procedures.
5. Social engineering - The manipulation of people into performing actions that may lead to the exposure of sensitive data is important, since human error is one of the most frequent reasons for data breaches and leaks.

Blue team skills (To uncover backdoors and vulnerabilities most people don't even know about.)

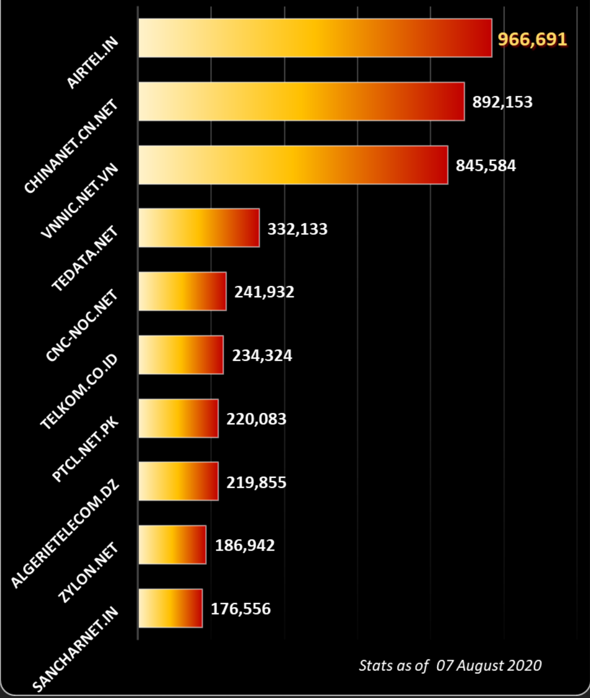
1. Organized and detail-oriented - Someone who plays more 'by the book' and with tried and trusted methods is more fitting as a blue team member. An extraordinarily detail-oriented mindset is needed.
2. Cybersecurity analysis and threat profile – Skills to create a risk or threat profile. A good threat profile contains all data that can include potential threat attackers and real-life threat scenarios. Make use of OSINT and all publicly available data.
3. Hardening techniques - To be truly prepared for any attack or breach, technical hardening techniques of all systems need to occur, reducing the attack surface hackers may exploit including the hardening of the DNS.
4. Knowledge of detection systems - Be familiar with software applications that allow tracking of the network for any unusual and possibly malicious activity. Following all network traffic, packet filtering, existing firewalls and such will provide a better grip on all activity in the company's systems.
5. SIEM Skills - SIEM, or Security Information and Event Management, is software that offers real-time analysis of security events. It collects data from external sources with its ability to perform analysis of data based on a specific criteria.

Conclusion - The entire cybersecurity industry needs to know more about engaging both teams to work together and learn from each other.

Find the complete article by SARA JELEN here: SecurityTrails

Worst Botnet ISP's by number of Bots

Source https://www.spamhaus.org/statistics/botnet-isp/



Stats as of 07 August 2020

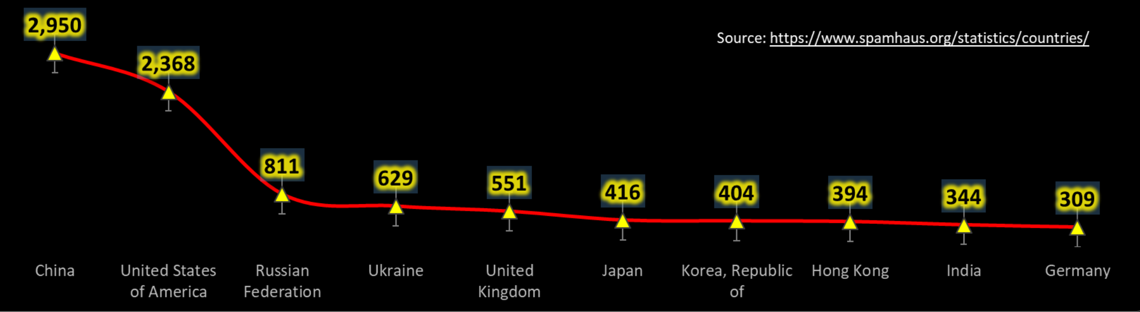
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Corona	Malware
1. Proper use of mask – Cover nose and mouth! 2. Wash mask regularly 3. A mask is worth nothing if not worn properly	1. Install proper Anti-Virus with real-time protection 2. Update regularly 3. Anti Virus is worth nothing if not maintained properly

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES) Data as on 07 August 2020

Source: https://www.spamhaus.org/statistics/countries/



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com