
**On October 21, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Juniper, SonicWALL, Magento, HP, Oracle, and Google 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

## 23 October 2020

## In The News This Week

### Hackers Donate Bitcoin From Ransomware Attacks to Charities

A group of hackers has donated some of the bitcoin it extorted via ransomware attacks to charities, claiming that it wants to "make the world a better place." However, the law says donations from ill-gotten gains must be rejected but charities have no way of returning donated bitcoin to the hackers. The group known as "Darkside" has surprised the world by donating a portion of the proceeds, the BBC reported Monday, adding that the group is relatively new on the scene. Darkside hackers claim to have extorted cryptocurrencies worth millions of dollars from companies. Claiming that they now want to "make the world a better place," the group donated 0.88 BTC, worth about $10,000, from their ransomware proceeds to two charities: The Water Project and Children International. their Read the full story here: Bitcoin

### Google's Waze GPS Navigation App Can Allow Hackers to Identify and Track Users

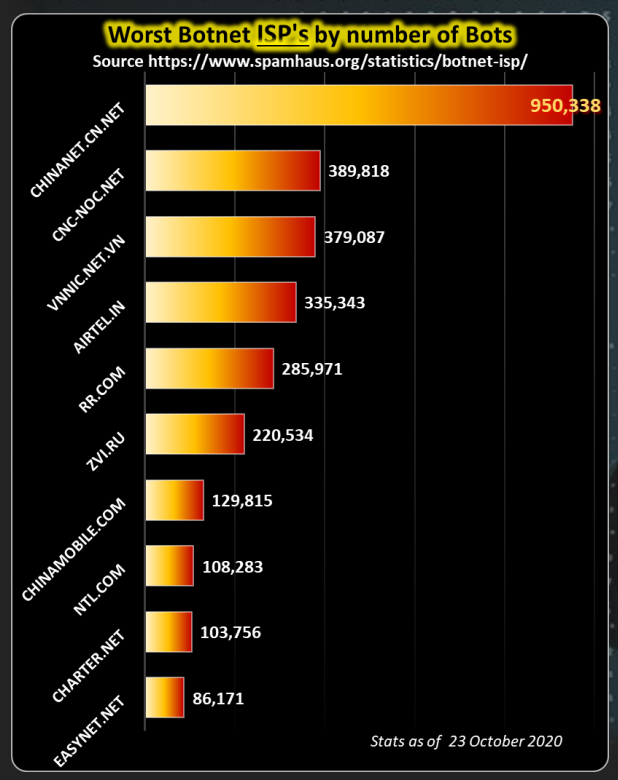
Google's Waze app contains a serious security vulnerability that allows hackers to identify users and track their locations. The flaw has since been patched and was an API flaw that allowed security researcher Peter Gasper to use the app to uncover the true identity of drivers using it. Gasper is a security DevOps engineer who found the API bug in the navigation software, finding that it allowed him to track the specific movements of nearby drivers in real-time. Gasper released details about the hack in a blog post uploaded to his research website. Google awarded Gasper a bug bounty of over a thousand dollars for uncovering the flaw after he reported it. Read the full story here: OODA *Loop*

### Microsoft says it took down 94% of TrickBot's command and control servers

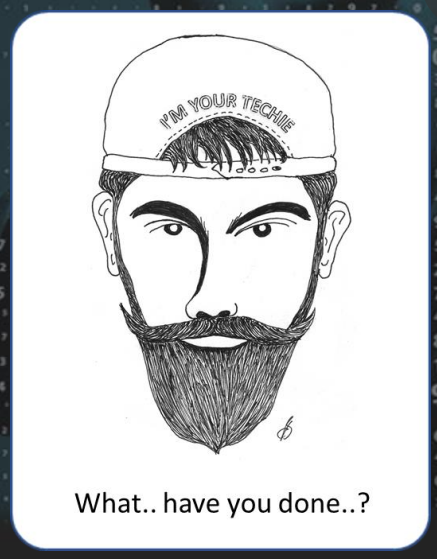
TrickBot survived an initial takedown attempt, but Microsoft and its partners are countering TrickBot operators after every move, taking down any new infrastructure the group is attempting to bring up online. Last week, a coalition of cyber-security firms led by Microsoft orchestrated a global takedown against TrickBot, one of today's largest malware botnets and cybercrime operations. Even if Microsoft brought down TrickBot infrastructure in the first few days, the botnet survived, and TrickBot operators brought new command and control (C&C) servers online in the hopes of continuing their cybercrime spree. But as several sources in the cyber-security industry told ZDNet last week, everyone expected TrickBot to fight back, and Microsoft promised to continue cracking down against the group in the weeks to come. In an update posted today on its takedown efforts, Microsoft confirmed a second wave of takedown actions against TrickBot. The OS maker said it has slowly chipped away at TrickBot infrastructure over the past week and has taken down 94% of the botnet's C&C servers, including the original servers and new ones brought online after the first takedown. Read the story here: ZDNet Article

### South Africa - Vodacom and MTN have not notified Information Regulator of location data breach

- Vodacom and MTN have yet to inform the Information Regulator of South Africa of the unlawful use of cellphone location data by Wireless Application Service Providers (WASPs) to track subscribers on their networks. This follows investigations into the murder of Lieutenant-Colonel Charl Kinnear, which revealed that criminals were able to track Kinnear's movements through his phone using location-based data and plan his assassination. Kinnear's assassination exposed the widespread abuse of location-based data to track the movement of South Africans without their knowledge or consent. This data is provided to companies by Vodacom and MTN. The Information Regulator confirmed to MyBroadband that cellphone location data is considered personal information, and it must be notified if there has been a security breach involving location data. "Section 22(1) and (2) of POPIA requires that responsible parties such as Vodacom and MTN notify the Information Regulator if there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person," the Information Regulator told MyBroadband. POPIA is the Protection of Personal Information Act of 2013. Read the story by Jan Vermeulen here: MyBroadband




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




## How AI Will Supercharge Spear-Phishing

AI (Artificial Intelligence) has been a hot topic for the last few months and the constant tug-of-war between the good and the evil uses of AI highlights the fact that both the bad guys and the good guys are anxious to make use of technology advances. In a DarkReading article this week, this "tug-of-war" is quite skilfully brought to light. Herewith a slightly adapted version. (Find the original article here: DarkReading)

To keep pace with intelligent, unpredictable threats, cybersecurity will have to adopt an intelligent security of its own. Imagine a strain of malware hidden on your colleague's computer. It watches their every move, quietly listening and learning as it sifts through their email, calendar, and messages. In the process, it doesn't just learn their writing style. It learns the unique way they interact with nearly everyone in their life. It picks up on the inside jokes they share with their spouse. It knows the formal tone they employ with their CEO. And it recognizes the familiar cadence they use with one of their most frequent contacts: You.

Their emails to you are often casual. And before important meetings, they are prone to sending you a friendly message of encouragement. One day, as you prepare for a morning meeting with a client, you get an email from them.
It reads:

> *"Hey.*
> *I'll see you at 9 for our call. You're gonna kill it today.*
> *See dial-in details for the call attached.*
> *Cheers,*
> *Al"*

Most people wouldn't question the legitimacy of this email – it's characteristically laid back and your email browser tells you it is from a trusted contact. But in reality, the attachment is a malicious payload that, if opened, would start rapidly encrypting data and hold your company's files hostage for a $30,000 ransom.

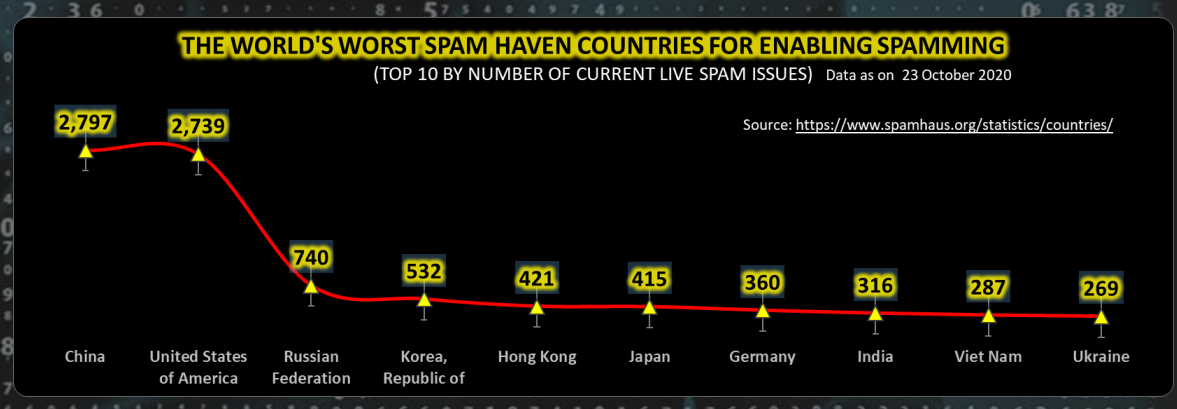
This example is hypothetical, but it's far from impossible. With the emergence of offensive artificial intelligence (AI), we are at the precipice of a new era of email attacks that move away from the low-grade attacks of yesterday, such as that long-lost relative explaining to you in broken English the large sum of inheritance you are owed. Today, we are moving toward a much more subtle and dangerous form of attack that masquerades as your most trusted contacts and blends into the daily noise of your digital interactions. As offensive AI emerges on the threat landscapes horizon, it becomes increasingly crucial for defenders to seek tools that can separate the signal from the noise.

**AI: The Good, the Bad, and the Ugly** - Artificial intelligence is influencing our lives in so many ways, from healthcare to smart cities. For example, BlueDot AI picked up on a cluster of "unusual pneumonia" cases happening around a market in Wuhan, China, and flagged it, nine days before the World Health Organization clocked it. It is now being used to crunch literature around the disease and its DNA in order to come up with the right medical compounds for a cure. Elsewhere, densely populated urban areas are using AI to mitigate traffic density and accidents. Sensors installed at parking lots, traffic signals, and intersections use AI to correlate data for the governments to plan their city initiatives. But AI won't just be used for good. Inevitably, it will also open the door for sophisticated cyberattacks like the threat spelled out above. Indeed, AI will supercharge spear-phishing with automated, intelligent technology. Hyper-realistic, machine-written copy is not some distant fiction. Rather, the technology required for this already exists today.

From Google's DeepMind to voice-recognition software like Amazon's Alexa, machines can now recognize and copy subtle patterns in human behavior. Recently, OpenAI's language generator, GTP3, autonomously wrote an entire, coherent article published in The Guardian on what it's like to be a robot. In the wake of these developments, an email from your colleague would be child's play for an even moderately advanced AI. Artificial intelligence won't just power phishing attacks either. It will augment every kind of cyberattack with adaptive decision-making capabilities. Automatically crafting a well-informed, well-written email containing a malicious payload is just the start; the inbox is simply a gateway into the organization. Once inside those gates, AI will supercharge every subsequent step of the attack kill chain – cracking even complex passwords in seconds, autonomously finding the optimal pathway to its final target, and exfiltrating only relevant, sensitive, and valuable documents at machine speed and stealth.

**Fight AI with AI** - To keep pace with intelligent, unpredictable threats, cybersecurity will have to adopt an intelligent security of its own. The legacy approach used by many email security vendors – which relies on predefined rules and signatures based on yesterday's attacks – is no longer sufficient in the age of offensive AI. These tools may catch spam and other low-hanging fruit, but in the face of advanced and novel email threats, they don't stand a chance. Cybersecurity firm Darktrace uses AI on the defensive side to gain a complex, nuanced, and continuously evolving understanding of each individual email user – learning how they behave, when and where they typically log in, and how they typically communicate. Rather than measuring an inbound email against a list of "known bads," it analyzes thousands of metrics around the email and asks, "Is this email unusual or anomalous?" This enables the technology, Antigena Email, to step in and decisively neutralize malicious emails that fall outside of the sender or the recipient's typical "pattern of life." Hundreds of organizations that have adopted this fundamentally new approach to email security have reported far higher catch rates, with advanced threats that slipped through traditional tools spotted and stopped before they reach the inbox. Darktrace's self-learning AI technology has already caught a range of creative attacks, from fake invoices claiming to come from a familiar supplier to an impersonation of a board member targeting several high-profile figures in an organization. With open source AI tools now at an attacker's disposal, these threats are only going to become increasingly advanced, making defensive AI an ever more vital technology.

Hackers are constantly looking to outsmart and outpace defenders, and they will no doubt harness the power of machine learning to supercharge their attacks in the near future. In the ever-evolving cat-and-mouse game between cybercriminals and security professionals, defenders must themselves adopt cutting-edge AI technology to stay ahead of the threats. (DarkReading Article)




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