BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle

June 2019

2019 Sees A Huge Rise In Ransomware Attacks

According to FBI statistics, in 2013 there were 991 tracked incidents of ransomware attacks against business, resulting in losses slightly exceeding half a million dollars.

The number of incidents steadily increased through 2016 when they reached 2,673 for the year, with total losses just shy of two and a half million dollars.

During the 2017-2018 period, the overall number of ransomware attacks declined from their high-water mark, even as the total losses continued to increase. This was a consequence of the hackers targeting larger networks with bigger payoffs. It led some to believe that interest in ransomware was beginning to wane in the hacking community in preference for other forms of attack.

That conclusion seems to have been premature. According to the statistics gathered so far for 2019, there has been an enormous increase in the total number of ransomware attacks. Businesses have borne the brunt of the surge, reporting an increase in excess of 500 percent. While there are no hard figures yet for the total damages, one can expect that the 2019 figures will be as record shattering as the total number of attacks themselves.

Of interest, in the same period, ransomware attacks targeting consumers is down markedly. They are down to the point that it's no longer even in the top ten most common cybercriminal threats that consumers face. That's good news for the consumer, but businesses are paying the price.

As a business owner, this is valuable information to know because if you are attacked, it's much more likely that the attack will come in the form of ransomware. Not to say you shouldn't be on your guard for other types of attacks, but give the reality of scarce IT resources, it pays to know what the biggest threats are.

Get More Free Tips, Tools and Services At Our Web Site

www.biz-net.com

(775) 850-7700

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

Report States Bots Account For 20 Percent Of Web Traffic

How much of the web's traffic would you estimate to be fake, if you had to guess? The answer to that question might surprise you. According to the 2019 Bad Bot Report published security firm Distil Networks, the answer is just over twenty percent. 20.4 percent to be precise.

More than one fifth of all traffic on the web is generated by bots.

As staggering as that figure is, it's actually down slightly from last year. Distil Networks says not to read too much into the slight dip, reporting that 75 percent of the bot traffic is generated by what it calls APB's, or Advanced Persistent Bots. APB's are able to cycle through IP addresses randomly carrying out whatever instructions their creators have outfitted them with. As these persistent bots become increasingly commonplace, we can expect their share of traffic to increase over time.

The report indicates, perhaps unsurprisingly, that the financial sector is on the receiving end of the majority of bot traffic. A full 42 percent of the bots are aimed at that sector alone, with the majority of this traffic driven by credential stuffing style attacks aimed at hijacking user accounts for financial gain.

Other popular bot traffic destinations included:

Ticketing portals, where 39 percent of all traffic was bot-driven
Education sites, where 38 percent of all traffic was bot-driven
Government websites, where 30 percent was bot-driven
Also unsurprisingly, the bulk of bot traffic (53 percent) originated in the United States, although Russia and the Ukraine accounted for nearly half of all blocking requests from Distil customers.

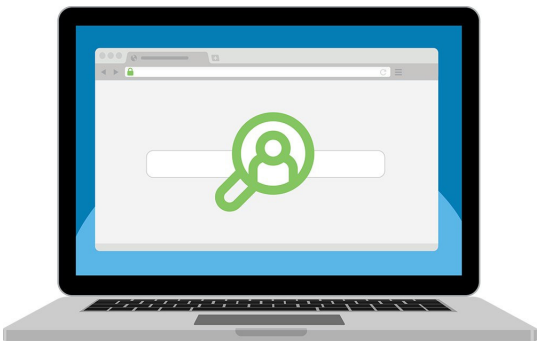
According to Tiffany Olson Kleemann, Distil Networks' CEO,

"Bot operators and bot defenders are playing an incessant game of cat and mouse, and techniques used today, such as mimicking mouse movements, are more human-like than ever before."

The bottom line is simply this: Bot traffic is bad for business. It costs you time and money, and it potentially puts your systems and your proprietary data at risk.

- The singular of spaghetti is spaghetto.
- The word karaoke is derived from two Japanese words karappo meaning 'empty' and okesutura meaning 'orchestra'.
- Google and Yahoo have both used goats to "mow" the grass at their corporate headquarters and datacenters.
- In 2007, Scotland spent over £100,000 (~$127,400 USD) changing their national slogan from 'The Best Small Country in the World' to a "vibrant" new slogan of 'Welcome to Scotland'.
- The 2008 Beijing Summer Olympics opening ceremony was watched by over a billion people. It's the first sporting event to reach that landmark viewership level
- In a two player game of Monopoly, there is a 12% chance that the game will go on indefinitely.
- In 2013, Hanukkah began on the same day as Thanksgiving. This won't happen again until the year 79811 AD.
- Over 500 hours of fresh video is uploaded to YouTube every minute.

Search Yourself Online



You most likely have heard how important it is to protect your privacy and the information you share online. To demonstrate this, we are going to try something new; we are going to show you how to research yourself and discover what information is publicly known about you. The process is called OSINT, a fancy way of saying Open Source Intelligence. This means researching public resources online to see how much information you can learn about a computer IP address, a company, or even a person like yourself. Keep in mind, cyber attackers are using these very same tools and techniques. The more attackers can learn about you, the better they can create a targeted attack. This concept has existed for years, but the latest online tools make it so much simpler to accomplish.

How to Find Information

You will not find all the information on a single website. Instead you start with one website, learn some details, then use those details to search on and learn from other sites. Then you combine and compare results to create a profile or dossier of your subject. A good place to start is with search engines such as Google, Bing, or DuckDuckGo. Each of these have indexed different information about you, so start your search with more than one search engine. Start by typing your name in quotes, but after that expand your search based on what are called operators. Operators are special symbols or text you add to your search that better define what you are looking for. This is especially important if you have a common name; you may have to add more information such as your email address or the town you live in. Learn more about operators and advanced search techniques in the Resources section at the end. Examples include:

- "FirstName LastName" > What information can I find online about this person
- "Firstname Lastname@" > Find possible email addresses associated with this person
- "Firstname lastname" filetype:doc > Any word documents that contain this person's name

There are also sites dedicated to learning about people. Try one of these sites to see what is publicly known about you. Keep in mind these sites are not always accurate or may be country specific. You may have to search several sites to verify the information you find.

- https://pipl.com
- https://cubib.com
- https://familytreenow.com
-

Finally, there are numerous other sites you can search to learn more, such as Google Images, Google Maps, social media sites, and many others. For an interactive list of all the different websites you can use to learn about yourself, we recommend the OSINT Framework at https://osintframework.com.

How to Protect Yourself

1. Learn what other people or organizations have collected, posted, or shared about you online (churches, schools, sports clubs, or other local community sites).
2. Understand that these same resources are available to anyone else, including cyber criminals who can use that information to target you. Be suspicious. For example, if you get an urgent phone call from someone claiming to be your bank, just because they know some basic information about you does not prove it is your bank. Instead, politely hang up, then call your bank back on a known, trusted number to confirm it is them. It is the same with email, just because an email has some known facts about you does not mean it is legitimate.
3. Consider what you share publicly and the impact that information could have on you, your family, or your employer.

Device Maintenance 101

Device Hygiene Explained

As with automobiles, buildings, and our own bodies, devices require a bit of maintenance. Failing to take basic proactive steps, such as updating apps and deleting and organizing files, can lead not only to degraded performance, but also adds security risks. Here at work, it's your responsibility to follow our organization's policies which are aimed at proper device maintenance. If you're unsure of those policies, please ask! And don't neglect your personal devices. A small commitment to device hygiene yields reliable functionality and reduced security risks.

APPS TO CONSIDER

Keeping your machines clean and running properly doesn't require a ton of work. Here are a few great tools that can help you live a healthy cyber life. As always, never install third-party apps on work-issued devices unless policy allows.

PASSWORD MANAGER

Having trouble remembering all of the logins for all of your accounts? Get a password manager! It creates, stores, and syncs your usernames and passwords across multiple devices.

VPN

Short for virtual private network, a VPN encrypts your internet traffic to prevent cybercriminals from intercepting and stealing your data on public WiFi networks.

ANTIVIRUS

One of the most inexpensive and basic options, software that prevents viruses or malware should be utilized on desktops and devices alike.

FIND MY PHONE

Most smartphones offer a service that allows you to locate your phone from a different device and ping it to ring or completely reset it to default, which erases all sensitive data.

AUTHENTICATOR

Two-factor authentication, or 2FA, requires something you know (your password) plus something you have (your phone) in order to log into an account. Authenticator apps improve on traditional, less secure 2FA methods such as sending codes to your phone number or email address.

Smartphone Security Checklist

- ☐ **Remove unused apps** *(digital cleaning)*
- ☐ **App permissions reviewed** *(not everything needs access to your location)*
- ☐ **Antivirus software installed** *(it is a computer, after all)*
- ☐ **Password protected and lock screen after a short period of no use** *(it is simple common sense)*
- ☐ **VPN installed** *(never connect to public WiFi without one)*
- ☐ **Auto update enabled** *(updates often patch security flaws and glitches)*
- ☐ **Backed up** *(either to the cloud, a computer, or both)*