**IBM Security**

August 2015

# IBM X-Force Threat Intelligence Quarterly, 3Q 2015

*With attacks by ransomware on the rise, it's more important than ever to understand how malware travels the Internet and infects networks.*

# Contents

# Executive overview

Our report this quarter opens with a discussion of ransomware. The media tends to cover data breaches more often than ransomware incidents, but ransomware presents a growing threat. The FBI estimates that just one ransomware threat, CryptoWall, has so far netted its operators about USD18 million.[1] Even law enforcement organizations have fallen victim.[2] As the sophistication of the threats and attackers grows, so does the targeting of their operations, to the extent that some attackers specialize in ransoming the local data files of popular online games. The evolution of these threats follows a pattern we have seen before, becoming more available to more attackers. Already, "ransomware as a service" offerings have started to appear, just as exploit kits before them provide "infection as a service." The IBM® X-Force® team suspects that this may be the beginning of a long battle for all of us.

The Dark Web hiding under the covers of the web we all know and love comes under scrutiny in our next article. As in the unknown depths of the oceans, the Dark Web remains largely unknown and unexplored, and it also hides predators. The recent experience of IBM Managed Security Services (IBM MSS) shows that criminals and other large-scale threat actors employ The Onion Router (Tor) software that enables anonymous communication as both an attack medium and an infrastructure for botnet command and control. The design of routing obfuscation in the Tor network provides illicit actors with additional protection for their anonymity. It can also obscure the physical location from which attacks originate, and it allows attackers to make the attack appear to originate from a specific geography.

Tor itself provides the focus of our third article. This article reiterates the conclusions of previous IBM MSS articles, and offers additional technical details needed to protect your corporate networks against both malicious and unintentional threats presented by Tor.

The final article in this report takes a quick look at vulnerability disclosures so far this year and closes with an overview of the changes in the Common Vulnerability Scoring System (CVSS) v3.

# Ransomware as a service

## Ransomware is not what it used to be. Today's ransomware constantly evolves and demands attention as well as protection.

Ransomware as a malware category has been around for a while. Over the years, it has been known by different names, such as "scareware" in the case of earlier, less destructive versions. Over time, ransomware has become big business that nets criminals millions of dollars a year. For example, a campaign known as CryptoLocker reaped an estimated USD1 million in six months.[3] And CryptoWall netted USD18 million since it first appeared about 2013.[1] So far, the victims have primarily been end users, but as the X-Force team takes a closer look at how ransomware is evolving, we observe that the technical sophistication is increasing as ransomware also begins to specialize, targeting specific communities.

In its earlier modern incarnations, such as WinLocker, ransomware merely "locked" the computer by displaying a scary message and making it difficult to bypass the screen to run other applications. For advanced computer users, it almost seems comical that users could be fooled by the appearance on a user's computer of a warning (purportedly) from a law enforcement agency such as the FBI requesting money. However, there are circumstances under which someone might be fooled or pay anyway.

A surprising number of users are fooled by fake/rogue anti-virus (AV) messages that are nothing more than animated web ads that look like actual products. The fake AV scam tricks users into installing or updating an AV product they may never have had. Afterward, the fake AV keeps popping up fake malware detection notices until the user pays some amount of money, typically something in the range of what an AV product would cost. Returning to the WinLocker example, some users who are not fooled may still decide that the infection is not worth the time and effort to remove on their own, and they may just pay up to move forward.

The creators of subsequent ransomware, including CryptoLock, ZeroLocker and CryptoWall, decided to take their methods further by encrypting the contents of the hard disk and requiring a ransom to be paid. The ransomware accomplishes this through public key cryptography where they either generate a key pair or obtain the public encryption key from their command-and-control server. While the earlier WinLocker and its clones primarily relied on proprietary web-money products such as Ukash, the subsequent generation of ransomware adopted cryptocurrencies, primarily Bitcoin. In some cases, Ukash equivalents and Bitcoins are accepted for ransom payments and other times just Bitcoins. Cryptocurrencies provide attackers a significant advantage: anonymity. The more advanced criminal networks have myriad ways to cope with the cash-out process and remain anonymous or semi-anonymous.

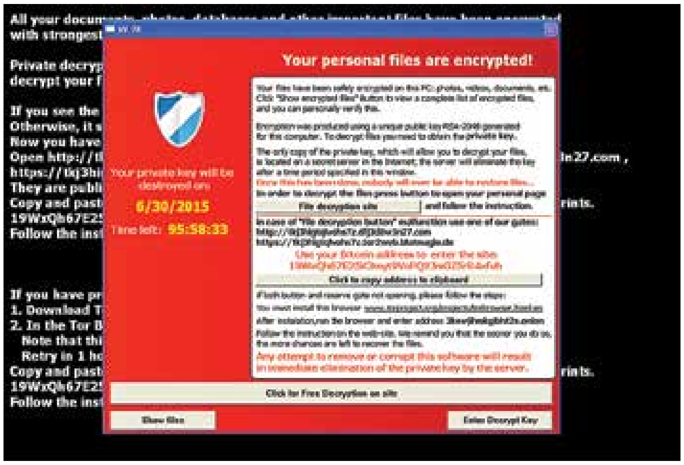
CryptoLocker was relatively easy to stop because it phoned home to its command-and-control servers before the destructive activity of encrypting the hard disk. This is despite the fact that the authors used pseudo-random domain names for the command-and-control servers generated by a domain generation algorithm (DGA) that produced a thousand domains per day. However, there was a flaw in that before the DGA was executed, CryptoLocker attempted to contact a static domain. The DGA approach to generating IP addresses is increasingly common; however, even knowing the domains it will generate, sometimes it is not practical to preemptively "sinkhole" the generated domains. By preventing the phone home operation, you can avoid the subsequent stages of CryptoLocker infection, which create the opportunity for traditional anti-malware solutions to get updates with infection removal capabilities.

The same event flow has been seen in CryptoWall, but not in subsequent ransomware such as CTB-Locker and ZeroLocker. As a result, updating protection is an important step—but it is not the only measure you should take. The success of ransomware underlines the importance of backing up your data so you always have access to it, even in the face of attack.

## Protecting yourself from possible infection

As a computer user, you always have the potential for hardware failures—and in many, if not most, cases, you can recover from these issues. But destructive malware such as modern ransomware is another story. Do not assume that if you are infected with encryption-based ransomware you can simply pay the ransom and reliably get your data back. For example, ZeroLocker command-and-control servers that have not been properly configured may never have received your encryption key, so they *can't* sell your data back to you. As a result, they are not only stealing your data, they can't give it back to you even if you pay! In addition, the authorities or a competing threat group may have "taken down" the command-and-control servers between the time your machines get infected and the time you try to pay the ransom. Similarly, there can be still other buggy circumstances that prevent data recovery. Again, the best way to avoid loss is to back up your data.

Regardless of whether your backup is local or cloud-based, you must ensure that you have at least one copy that is not directly mapped visibly as a drive on your computer. Some ransomware variants will target any drive that is mounted, whether it is mapping to a physical hard drive, a USB flash drive, a network drive or a cloud-based service. In the case of a cloud storage service mapped to a drive, the chances are good that you can recover an earlier version of the file, but it may be a hassle to recover many files. Further, it is not safe to assume the kinds of files the ransomware will target for encryption. Many look for a wide range of file types; others go after specific types. TeslaCrypt, for example, targets online gamers by going after the user files related to online games. It is only a short jump to see how proprietary file formats that relate to particular communities might be attractive to attackers.



All your docum
with strongest

Private decryp
decrypt your f

If you see the
Otherwise, it s
Now you have
Open http://t
https://tkj3hi
They are publi
Copy and past
19WxQh67E2
Follow the inst

If you have pr
1. Download T
2. In the Tor B
Note that thi
Retry in 1 ho
Copy and past
19WxQh67E2
Follow the inst

Your private key will be destroyed on:

6/30/2015

Time left: 95:58:33

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files press button to open your personal page File decryption site and follow the instruction.

In case of "File decryption button" malfunction use one of our gates:
[illegible]
[illegible]

Use your Bitcoin address to enter the site:
[illegible]

If both button and reserve gate not opening, please follow the steps:

You must install this browser [illegible]

After installation,run the browser and enter address: [illegible]

Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Click to copy address to clipboard
Click for Free Decryption on site
Show files
Enter Decrypt Key

*Graphic 1. TeslaCrypt ransom screen*

## Ransomweb attacks evolve

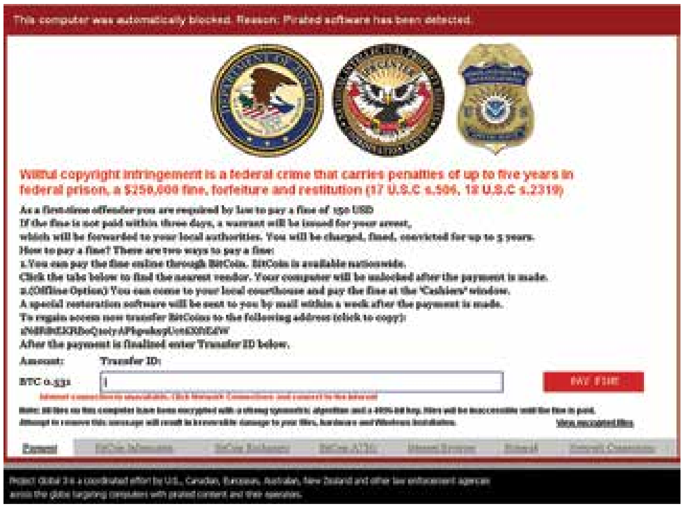
As defenses take different approaches, new attack opportunities arise, technology changes, and attack mechanisms—including ransomware—evolve. In December 2014, experts at High-Tech Bridge started to observe what they call "ransomweb" attacks.[4] In this flavor of ransomware, ransomweb targets web application owners rather than individual end users by inserting code on vulnerable web servers. These web applications rely on databases to provide information including login credentials, such as user names and salted, hashed passwords. In this attack scenario, the data stored is encrypted without anyone noticing, leaving an unencrypted database full of data in an encrypted state. The decryption key is provided for some amount of time to ensure normal operations before it is suddenly yanked and the web applications cease to function or function improperly. Shortly thereafter, a ransom note is sent. Victims of this scam so far have been limited to an unnamed financial services company and a couple of online message boards.

Ideally, such an attack could be prevented by the difficulty of compromising a website to execute a ransomweb attack. However, many web application vulnerabilities exist. Though prevention methods are known for most of them, these are a leading category among the vulnerabilities that are disclosed every year.[5] Additionally, users continue to utilize unsafe practices such as reusing passwords.

## The VirLock ransomware

In a nasty turn of events, another newer ransomware originally discovered in late 2014, VirLock, will not only encrypt a variety of different files but will also turn them into file infections. The VirLock ransomware creates copies of itself, with small changes, for every file it infects. For content such as images and movies, the malware will replicate the icon image and the file path information but add a permutation of the malware and an encrypted form of the original content, plus an executable suffix such as “image.jpg.exe” for instance.

This is interesting in that it not only occurs without the need to contact a remote command-and-control server, but re-infection and/or spreading of the infection is relatively easy if the infection is not totally cleaned up. Let’s say you have a removable drive connected, such as a USB drive or a cloud storage drive mapped to a drive letter. Both are targets, and infections could be spread by either. In practice, the alert notification occurs quickly enough that removable storage might be impacted but the end-user may realize that it is a bad idea to do anything further without help. Especially in the work environment, it is best to get help from IT security or a similar team as soon as an infection is observed.



This computer was automatically blocked. Reason: Pirated software has been detected.

Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)

As a first-time offender you are required by law to pay a fine of 150 USD
If the fine is not paid within three days, a warrant will be issued for your arrest,
which will be forwarded to your local authorities. You will be charged, fined, convicted for up to 5 years.
How to pay a fine? There are two ways to pay a fine:
1.You can pay the fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest vendor. Your computer will be unlocked after the payment is made.
2.(Offline Option) You can come to your local courthouse and pay the fine at the 'Cashiers' window.
A special restoration software will be sent to you by mail within a week after the payment is made.
To regain access now transfer BitCoins to the following address (click to copy):
[illegible]
After the payment is finalized enter Transfer ID below.

Amount: Transfer ID:
BTC 0.531

Internet connection is unavailable. Click Network Connections and connect to the Internet

Note: All files on this computer have been encrypted with a strong symmetric algorithm and a 4096-bit key. Files will be inaccessible until the fine is paid.
Attempt to remove this message will result in irreversible damage to your files, hardware and Windows installation.

Project Global 3 is a coordinated effort by U.S., Canadian, European, Australian, New Zealand and other law enforcement agencies across the globe targeting computers with pirated content and their operators.

*Graphic 2. VirLock ransomware message*

## From simple to elaborate, scams will continue

We are observing the start of a prolonged battle with ransomware, as ransomware attacks diversify from simple scams to more elaborate ones that target high-value communities or businesses. Even where the scams may target the general user base, the attacker may simply have purchased access to the infrastructure necessary for the attack and contracted with the supplier of the infrastructure and ransomware for its use. Such an attacker does not continue to have a direct relationship with the infrastructure following the attack.

Tox, a ransomware-as-a-service kit, was discovered in the wild by Intel Security this year (2015).[6] In much the same way that web browser exploit kits evolved to sales of exploit kits as a service, the arrival of ransomware as a service means attackers do not need to be technically sophisticated to utilize Tox. This simplicity may spread rapidly to more sophisticated but less common ransomware attack paradigms and lead to off-the-shelf offerings in the cloud. Various technical innovations and twists are likely to continue, leading to increasingly clever extortion schemes and growing financial losses. X-Force will be keeping an eye on ransomware as it continues to evolve.

# The Dark Web

## Today's sophisticated threats don't always arrive via the Internet we know well and use every day. They often take a deeper, darker path.

The US government helped create The Onion Router (Tor)[7] and partially funds ongoing development, largely because several parts of the US government use the Tor network. At the same time, governments and law enforcement agencies across the world try to break into the Tor network, and the US National Security Agency (NSA) allegedly uses Tor traffic as a signal that a subject should be intensely surveilled. Why? Because a lot of people use the Tor network to obscure their activities. Some are whistleblowers or citizens of repressive regimes with (allegedly) "pure" motives. Others are state actors, intelligence operatives, cybercriminals and other criminals with less wholesome goals. Together, these good and nefarious individuals and organizations comprise the Dark Web.[8]

IBM Managed Security Services (IBM MSS) recently dug more deeply into this topic, and you can read more about this report published here.

### Sometimes used by malicious actors, Tor began to protect legitimate communications

Tor was originally designed, implemented and deployed in 2004 as a third-generation onion routing project of the US Naval Research Laboratory to protect government communications. Today, it is used every day for a wide variety of purposes by civilians, the military, journalists, law enforcement officers, activists and many others.

Because Tor enables anonymous communication, however, it has also been utilized for nefarious purposes. The purveyors of ransomware and other malware have found its ability to provide encrypted communication from host to host useful. Tor can serve as a proxy with exit points known as "exit nodes" to allow users to anonymously browse web pages externally to the World Wide Web. This offers moderate anonymity to anyone looking to hide their identity as well as encrypt communication back to their host computer or device.

### Exit nodes

Exit nodes present the "face of Tor" to the rest of the Internet in many ways. The Tor client software encrypts messages multiple times and injects them into the Tor network. As the message traverses the network, each intermediate Tor node removes one level of encryption. The Tor network identifies the node that removes the final layer of encryption as the *exit node*. That node assumes the responsibility of forwarding the request to the destination, receiving any response and injecting that response back into the Tor network for transport to the original requestor.

Creating Tor exit nodes is simple. With a spare computer, a copy of a Linux distribution and a couple of software downloads, you, too, can host a Tor node. In part, the ease of node creation originates with the desire of the US government for more people to use the Tor network—hiding the government's own use of it. If all of the traffic on Tor originated from US government, military and intelligence users, the use of Tor would implicitly brand the users as members of those communities.

The ease of creating a new Tor node, though, can have complex consequences for astute security operatives. Once a node is deployed, operators have little control over the traffic this simple, new node supports. That traffic can open doors to liability issues associated with content issuing from that node as well as resource consumption issues for the operators of the network hosting a Tor node. Further, the ease of setup that promotes widespread use also makes it easy for staff to surreptitiously deploy Tor nodes in their employers' networks, something IBM MSS has encountered often while investigating customer incidents. Finally, some malware silently installs Tor client software on infected hosts to obscure the command-and-control operations of the campaign, and some malware installs Tor node software to provide new exit or interior nodes on the Tor network.

Those wishing to use the Tor network for nefarious purposes show understandable reluctance to deploy or host exit nodes on their own equipment or networks. This reluctance grows from the same concerns as those held by corporate network operations personnel. First and foremost, the owner of an exit node can become legally liable for the content issuing from that node. This liability can include everything from being blacklisted by organizations such as the Real-time Blackhole List (RBL), to receipt of Digital Millennium Copyright Act (DMCA) takedown notices, to criminal prosecution and civil forfeiture, even if the content belongs to someone else and is hosted somewhere else. In addition, openly operating an exit node directly compromises the very anonymity of the node operator that the Tor network was created to maintain.

## Tor and geolocation

Another capability for anonymity enabled by Tor and its network involves disguising the geographic location of the requestor. The Netherlands and the United States host more Tor exit nodes than any other countries, including numerous high-bandwidth exit nodes. However, the Tor network encompasses exit nodes in many different countries. Figure 1 gives an idea of the geographic distribution of Tor exit nodes for the top 11 countries.

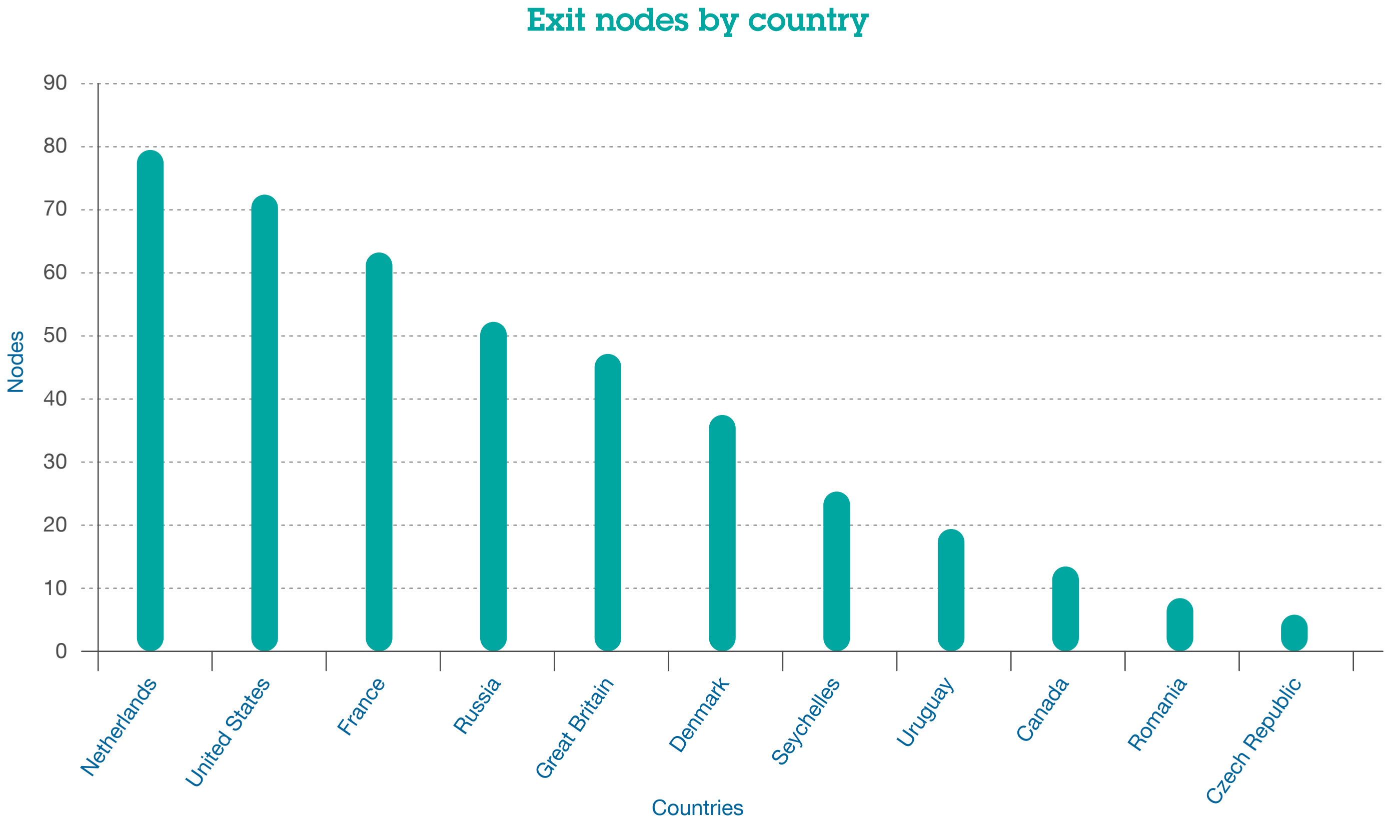


*Figure 1. Based on the geolocation of IPs used by exit nodes, the Netherlands is home to the largest number of non-malicious and malicious nodes combined*

Source: IBM MSS data (Jan 1, 2015 - May 10, 2015).

Tor clients choose the exit node to which the network will direct a message, before they inject it into the Tor network. Common Tor clients prioritize routes and exit nodes with higher bandwidth and lower load. These exit nodes also convey the highest volumes of malicious traffic originating from the Tor network, though the traffic patterns shift over time.

However, judicious selection of exit nodes by the Tor client can cause the traffic to appear to originate from a geography other than the one actually inhabited by the sender. Out-of-region seekers of region-controlled movies, for example, can use this capability to access media outside the control of the region-coding scheme. And from the perspective of an attacker, this capability can make the traffic *not* appear to come from a particular geography, a practice that can benefit espionage operatives, data thieves, or others with a desire to disguise their physical location. It can also be used to guide attacks under the radar of the defensive staff: a US retailer, for example, typically will find traffic from the US less suspicious than traffic from the other side of the world.

The IBM MSS global threat database provides a very unique view into the traffic that sources from Tor, as illustrated in Figure 2.

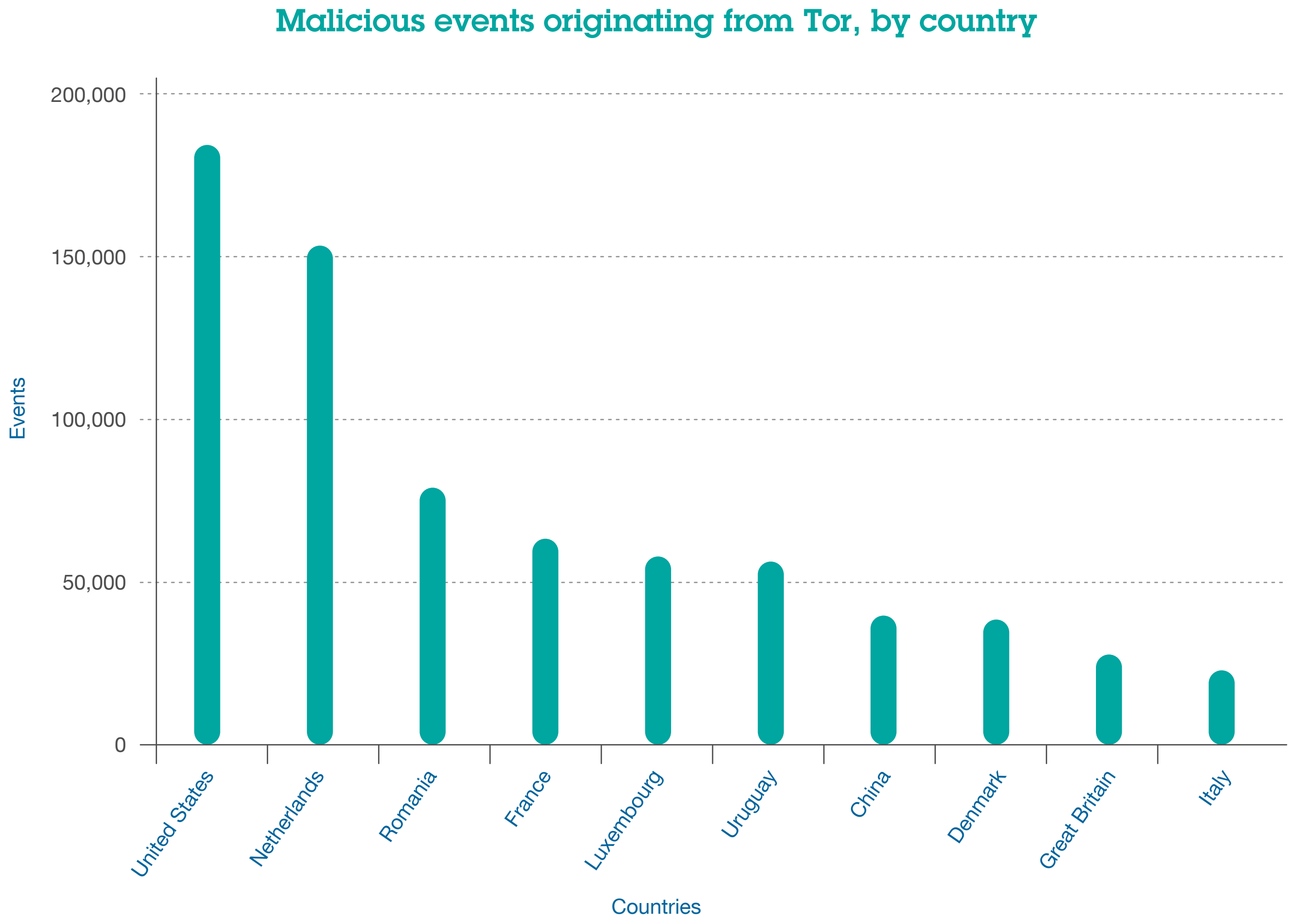


*Figure 2. Malicious traffic volumes sourcing from Tor exit nodes, by country*
Source: IBM MSS data (Jan 1, 2015 - May 10, 2015).

The list of industries targeted for attacks from Tor exit nodes also presents an interesting perspective illustrated in Figure 3. Based on traffic monitored by IBM MSS, these attacks target information and communications companies foremost, followed by manufacturing, then finance and insurance. This ranking at first appears to confound common wisdom. One might well expect finance and insurance to lead, based on the financial information targeted by well-known data breaches and media reports of financial theft based on them. But combining attacks on information and communications with manufacturing accounts for about three times as many attack events as finance and insurance. A likely explanation is that these attacks are not after money—they're attempts to steal intellectual property and/or spy on company operations.

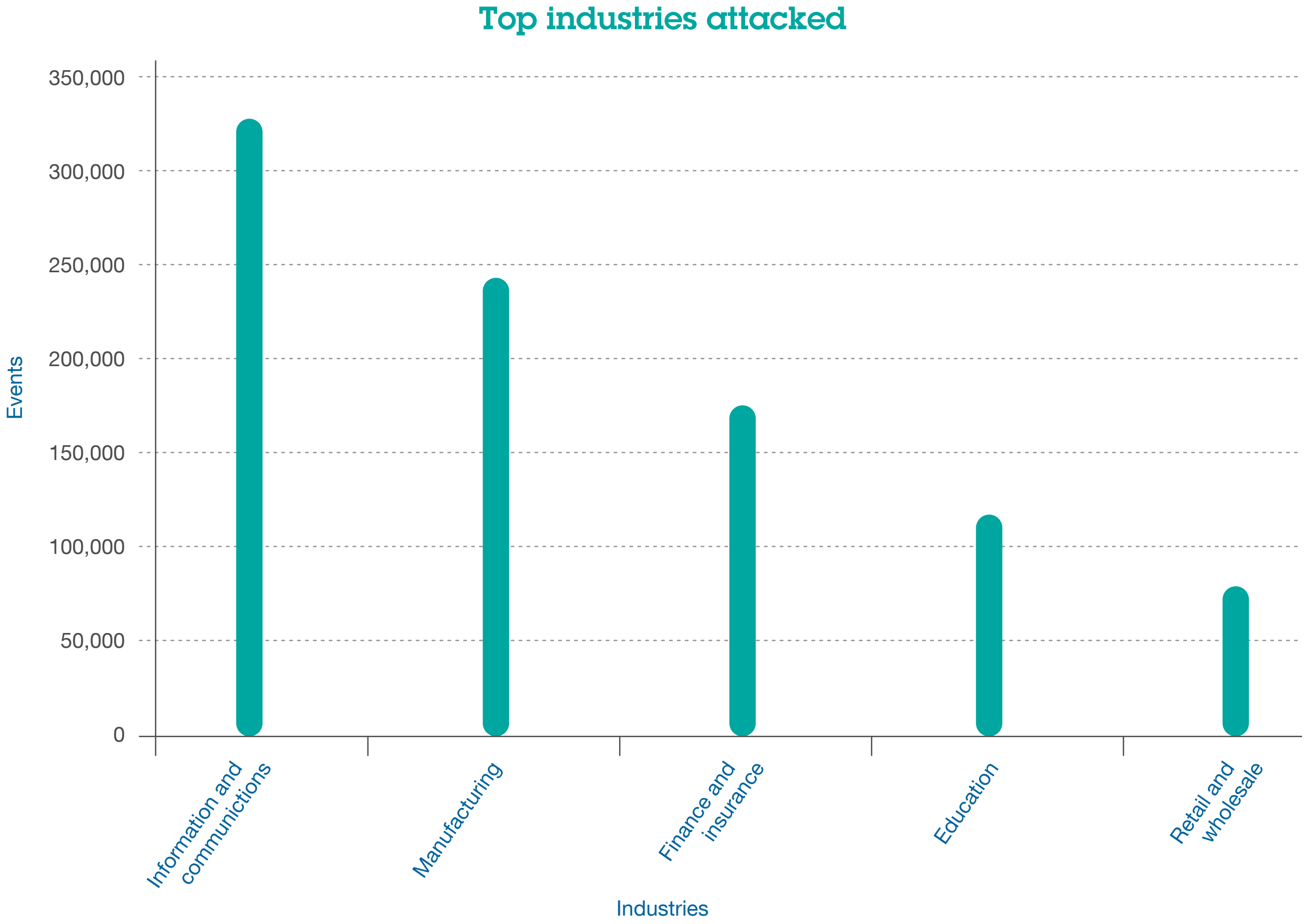


*Figure 3. More than 50 percent of malicious Tor traffic targets the Information and communications, and Manufacturing industries*

Source: IBM MSS data (Jan 1, 2015 - May 10, 2015).

## Tor as attack infrastructure

IBM MSS data shows a steady increase over the last few years in a variety of attacks originating from exit nodes of the Tor network. It appears that more malicious actors each year avail themselves of the anonymity of the Tor network. In particular, spikes in Tor traffic can be directly tied to the activities of malicious botnets that either reside within the Tor network or use the Tor network as transport for their traffic.

## Common attacks from Tor

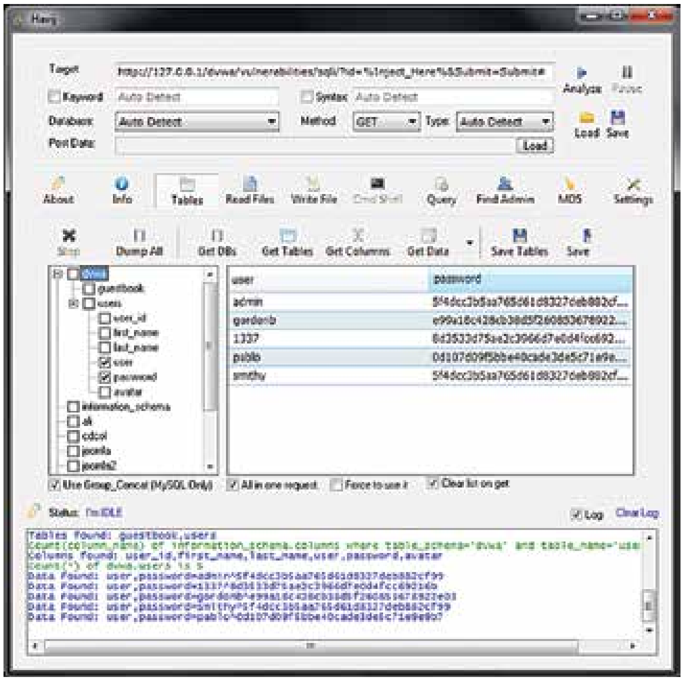
IBM MSS actively monitors Tor exit nodes to identify attacks originating from the Tor network. This data reveals some interesting patterns in the common Tor-sourced attacks.

### *SQL injection*

The old enemy SQL injection (SQLi) makes up by far the majority of the attacks that originate with Tor exit nodes to target IBM MSS customers. In part, this occurs because common Tor nodes are designed primarily to deal with HTTP traffic. It also occurs, however, because SQLi, even in 2015, still represents a lucrative attack. After all these years, the world continues to create websites vulnerable to SQLi. Aggravating an already bad situation, malicious tools like Havij provide easy-to-use, point-and-click interfaces to create SQLi attacks, further reducing the skill required to succeed.

### *Vulnerability scanning*

The prevalence of vulnerability scanning attacks coming from the Tor network should surprise no one. Vulnerability scanning often represents the early stages of an attack, as the adversary attempts to assess the lay of the target's land. Using the Tor network, the surveilling party can cloak their origin and spread their probes out across the population of exit nodes, reducing the risk of drawing attention. Most modern intrusion detection and web application firewall systems can easily detect and report scans in progress, and block the source(s). Having a number of exit nodes participating reduces the chances of being blocked, and increases the chances of having another IP address on hand that isn't blocked.



Target: http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=%Inject_Here%&Submit=Submit#

□ Keyword: Auto Detect

□ Syntax: Auto Detect

Database: Auto Detect

Method: GET

Type: Auto Detect

Post Data:

- □ dvwa
  - □ guestbook
  - □ users
    - □ user_id
    - □ first_name
    - □ last_name
    - ☑ user
    - ☑ password
    - □ avatar
- □ information_schema
- □ ali
- □ cdcol
- □ joomla
- □ joomla2

| user | password |
|---|---|
| admin | 5f4dcc3b5aa765d61d8327deb882cf... |
| gordonb | e99a18c428cb38d5f260853678922... |
| 1337 | 8d3533d75ae2c3966d7e0d4fcc692... |
| pablo | 0d107d09f5bbe40cade3de5c71e9e... |
| smithy | 5f4dcc3b5aa765d61d8327deb882cf... |

☑ Use Group_Concat (MySQL Only) ☑ All in one request □ Force to use it ☑ Clear list on get

Status: I'm IDLE

☑ Log

```
Tables found: guestbook,users
Count(column_name) of information_schema.columns where table_schema='dvwa' and table_name='use
Columns found: user_id,first_name,last_name,user,password,avatar
Count(*) of dvwa.users is 5
Data Found: user,password=admin^5f4dcc3b5aa765d61d8327deb882cf99
Data Found: user,password=1337^8d3533d75ae2c3966d7e0d4fcc69216b
Data Found: user,password=gordonb^e99a18c428cb38d5f260853678922e03
Data Found: user,password=smithy^5f4dcc3b5aa765d61d8327deb882cf99
Data Found: user,password=pablo^0d107d09f5bbe40cade3de5c71e9e9b7
```

*Graphic 3. The Havij interface makes SQLi incredibly simple to execute against targets*

### *Distributed denial of service*

Again, use of the Tor network for distributed-denial-of-service (DDoS) attacks should come as no surprise. These attacks combine Tor-commanded botnets with a sheaf of Tor exit nodes. In particular, some of the US-based exit nodes provide huge bandwidth. Employing a handful of the exit nodes in a DDoS orchestrated by the botnet controller and originating at dozens or hundreds of bot hosts can impose a large burden on the targeted system with small outlay of attacker resources, and generally effective anonymity.

## Mitigation

The dynamic nature of the Tor network increases the difficulty of protecting against these attacks, but does not make such defense impossible. Essentially, corporate networks must prevent traffic to and from stealth networks such as Tor. Though the Tor network is large, it is finite, and various frequently updated directories exist to identify Tor nodes, enabling wholesale blocking at the firewall. Application gateways and intrusion prevention system/intrusion detection system (IPS/IDS) solutions can flag attacks in real time and block further traffic from the source.

## Conclusion

Applications such as Tor can provide attackers significant leverage to further their goals, but do not by themselves leave a path of defeated defenders behind. Expect use of these services in attacks to expand and to make them somewhat harder to unravel—but take advantage of the mitigation capabilities outlined in this article.

Corporate networks really have little choice but to block communications to these stealthy networks. The networks contain significant amounts of illegal and malicious activity. Allowing access between corporate networks and stealth networks can open the corporation to the risk of theft or compromise, and to legal liability in some cases and jurisdictions.

# Controlling the use of Tor in corporate networks

## Without your knowledge, attackers may circumvent your controls and use your network to distribute malware. Take steps now to block these actions—and avoid financial or legal liability.

In the February 2015 *IBM MSS Threat Report*,[9] an article provided high-level information about Tor and its functionality. That article concluded that it is absolutely necessary to block access to Tor or other similar networks from your corporate networks. In this article we reiterate the conclusion, include some technical IP address information and suggest methods that attackers use for circumventing the Tor use prohibitions put into place to protect corporate networks. We conclude with suggestions for controlling the use of Tor in those networks.

### Circumventing IT controls

Before delving into methods used to circumvent controls over the use of Tor, a technical note is necessary:

Traffic on the Tor circuit is not encrypted until it reaches the first IP address ("hop") in the Tor circuit. However, in most deployments, the first hop is inside the originating computer, and the plaintext traffic never appears on the network until the exit node forwards it to the targeted host.

Some methods to circumvent Tor-control policies include:

- Use of a private subscribed proxy to access the Tor circuit
- Execute Tor from a USB device
- Use The Amnesic Incognito Live System (TAILS)

A privately subscribed, encrypted proxy can be launched to access the Tor circuit. If the user installed the proxy on a corporate machine, it's likely the traffic to the first hop (outside the corporate network) in the Tor circuit would be encrypted, thus concealing the traffic. However, the user could also install another Tor node in the company network, as well as a Tor proxy on the infected host. Then, (a) the plaintext never hits any network wire, and (b) when the packets cross the corporate perimeter, the actual miscreant is neither the sender nor the destination.

Executing Tor from a USB device would not require installation on the machine itself. Evidence of Tor use in this manner would be revealed only through a comprehensive forensic examination.

TAILS is a live, Linux-based operating system that can be used to boot a machine and directly connect to the Tor circuit by default, bypassing any local operating system functions. Once the TAILS instance is shut down, no evidence is left on the computer.

### Tor IP addresses

The February 2015 article provided a high-level explanation of the Tor circuit and functionality. At a more detailed level, the Tor circuit is made up of IP addresses from all over the world. The addresses are dynamic as old ones are repurposed and new ones emerge each day.

The web is replete with lists of Tor node IP addresses on various websites. These lists are updated constantly, sometimes every 30 minutes. Several sites provide script downloadable lists that can be used to compose your own deny or block lists.

In preparation for the article, IBM Emergency Response Services (ERS) downloaded various lists of Tor nodes from a number of websites over a period of three days.

One day we observed more than 6,600 total nodes (entry and exit) and the next day, there were approximately 5,000 total nodes. On a third day, the number varied again. Also available are lists of Tor exit nodes, which are also dynamic. A feature of some of these lists is the inclusion of the Tor version used on the node.

## IBM ERS Tor experience

IBM ERS detected the use of Tor IP addresses in several engagements in 2015. One engagement involved the use of the Tor circuit to launch brute-force password attacks on a customer's website. The attack resulted in the theft of reward points, and the subsequent redemption of those points cost the customer hundreds of thousands of dollars.

In the spring of 2015 there was an outbreak of ransomware across the US. In several engagements, IBM ERS uncovered the use of Tor sites to facilitate the Bitcoin payment of ransoms from victims of the outbreak. Thorough forensic investigation showed that the ransomware infections on computers were due to "drive-by" infections; a user simply accessed an infected webpage and was unknowingly infected with the ransomware. The infections and remediation resulted in the loss of hundreds of thousands, if not millions, of dollars in downtime and missed business opportunities.

## Tor relay hosting

An IT administrator might wonder who hosts Tor nodes and why this information is important.

As discussed previously, the simple answer to the "who" question is that anyone can host a Tor node. In a section of the Tor website, volunteers are requested to run a relay (an "interior node") to help the Tor network grow.[10] Volunteers can download the necessary software and run a Tor relay that allows any computer to act as a relay.

As for the "why," an administrator is unlikely to want someone to implement a Tor relay on network assets where the administrator has ultimate responsibility. In essence, running a Tor relay is a donation of bandwidth and an open door to several forms of liability. More important, if a Tor relay is running on a network, the administrator could be an unwilling facilitator of an attack on other networks or within his or her own networks.

## Recommendations to prevent the use of Tor

The first and most important recommendation for preventing Tor relays is the formulation and issuance of a comprehensive corporate policy for acceptable use.

Recommendations for formulating such a policy would include:

- Prohibiting the use of unapproved encrypted proxy services
- Prohibiting the use of personally subscribed proxy services
- Prohibiting the downloading and installation of unapproved software
- Prohibiting the use of personally owned removable devices such as USB, optical media and Secure Digital (SD) cards
- If the use of removable media is required, mandating the use of only company-approved devices
- Prohibiting the booting of corporate computers to any other media than the hard drive
- Altering the BIOS of computers to boot only to the hard drive
- Disabling autorun for removable devices
- Using publicly available lists of proxy nodes to block network traffic to and from those sites
- Implementing a comprehensive desk audit program to ensure compliance

In general, networks should be configured to deny access to websites such as www.torproject.org or any other sites associated with anonymous proxies or anonymization services such as Tor and The Invisible Internet Project (I2P). Users should be warned that accessing prohibited websites could result in disciplinary action.

# Vulnerability disclosures in the first half of 2015

## At present, the number of vulnerabilities has declined slightly, but there are indications their impact in the past may have been greater than originally estimated.

Since 1997, X-Force research has been tracking public disclosures of vulnerabilities in software products. The team tracks software advisories from vendors, monitors community mailing lists and public forums, and analyzes vulnerability reports where remedy data, exploits and vulnerabilities are disclosed.

In the first half of 2015, we reported just over 4,000 new security vulnerabilities. If this trend continues throughout the rest of the year, the total projected vulnerabilities would be about 8,000—the lowest total since 2011.

However, 2014 reflected a similar pattern, right up to the moment when the CERT Coordination Center of the Software Engineering Institute at Carnegie Mellon University disclosed the results of their Tapioca testing for which there seem to remain unanswered questions.

### Common Vulnerability Scoring System v3

In May 2012, the Board of Directors of the Forum of Incident Response and Security Teams (FIRST) selected IBM as one of the security vendors to participate in the creation of v3 of the Common Vulnerability Scoring System (CVSS).[11] Other industries such as finance, government and academia were also

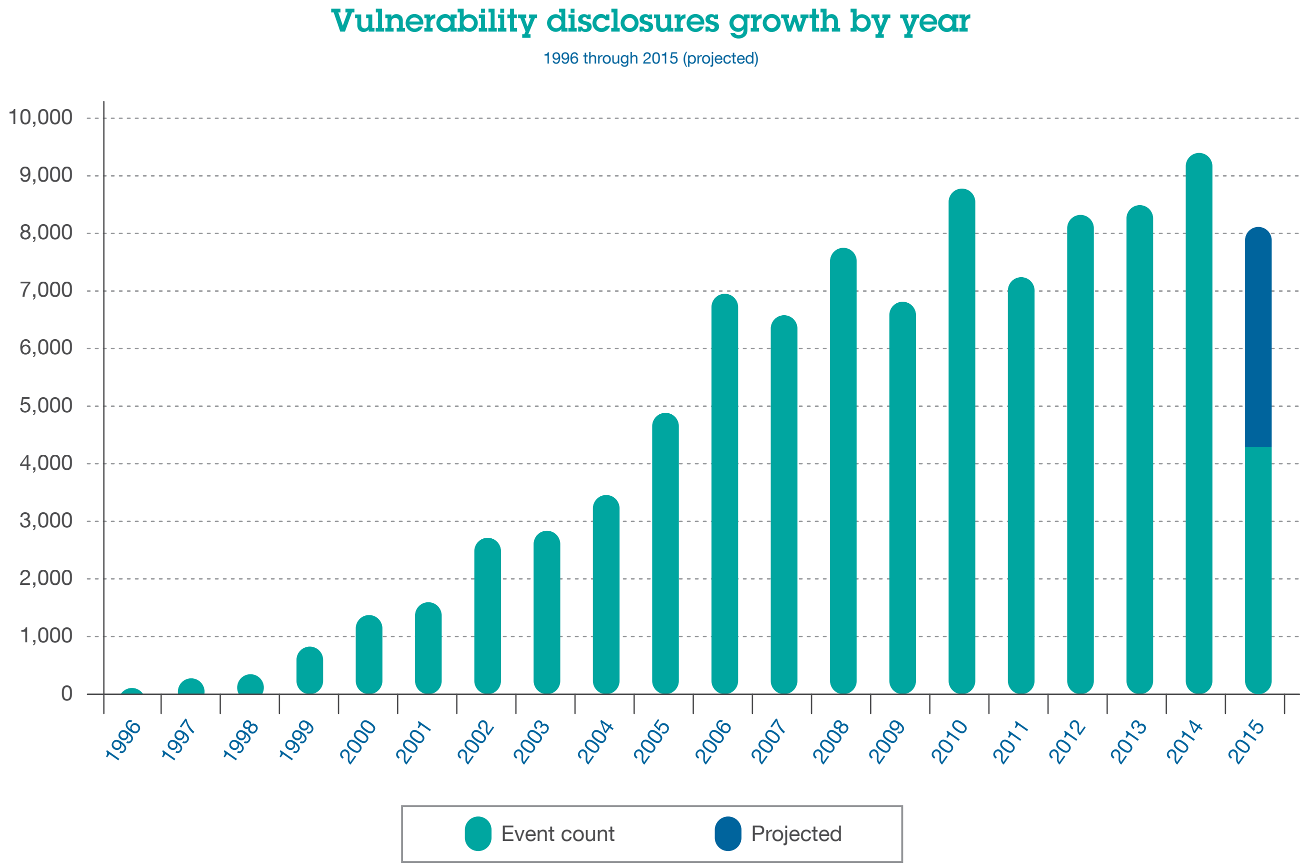


*Figure 4. Vulnerability disclosures growth by year, 1996 through 2015 (projected)*

tapped to work alongside the security industry to improve and expand on CVSS v2.

A base metric called *"Scope"* was added to v3 to address instances in which a vulnerability impacts a component other than the vulnerable component. In addition, the *"Impact"* vectors were enhanced to take into account when sensitive systems or information are affected.

A good example of a vulnerability that was reassessed by the CVSS v3 scoring is CVE-2008-1447, or the so-called DNS cache-poisoning "Kaminsky Bug." This DNS protocol vulnerability can be exploited to change a DNS record so that a given domain redirects to an alternate and potentially malicious IP address.

Under CVSS v2 this vulnerability was rated a 5.0 score, but under v3 the score was increased to 6.8. The increased score is attributed to the change of scope, where the vulnerable component is the DNS server and the impacted component is the end user or victim who connects to the server. Under v2, the wider reaching consequences of this change of scope were not factored into the scoring.

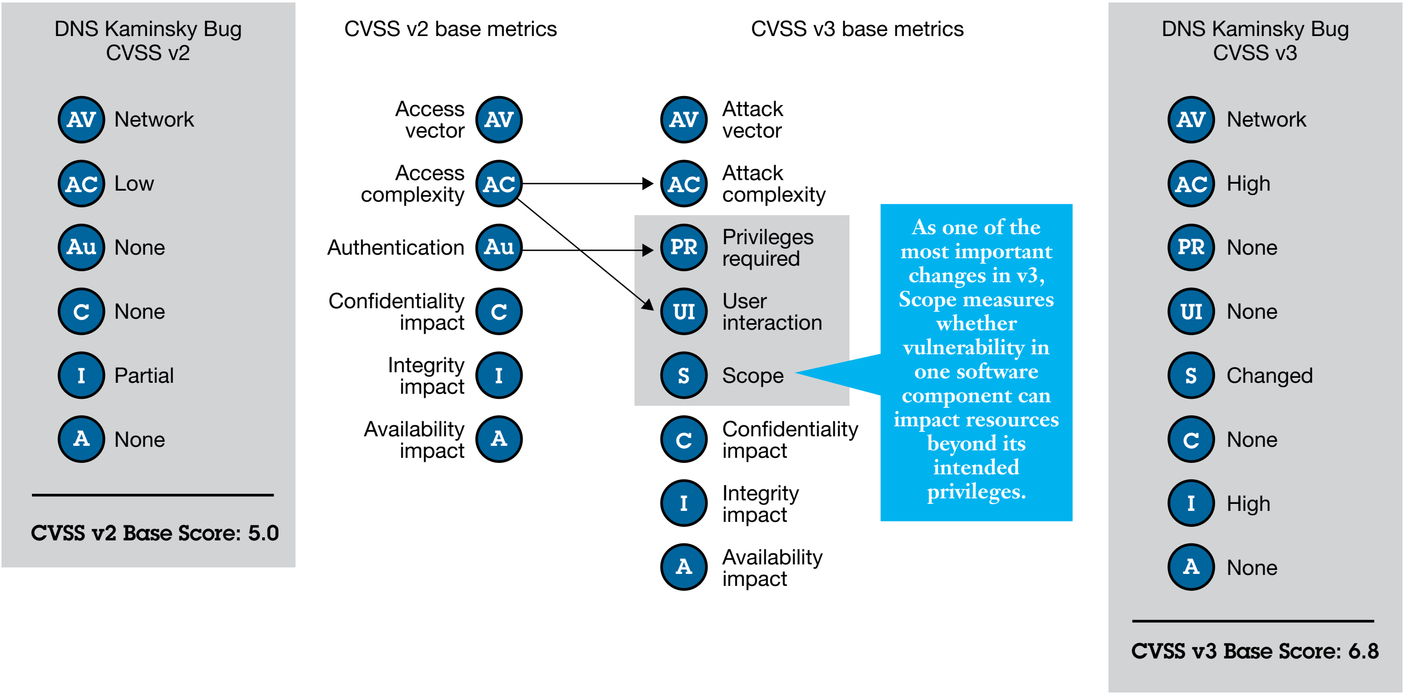
Another pertinent example is the Heartbleed OpenSSL vulnerability, which went from a medium severity score of 5.0 under the old criteria, to a high severity score of 7.5 under the new. In this case, a reassessment of the confidentiality impact from "partial" to "high" was a contributing factor in the increased risk score.

IBM formally adopted CVSS v3 on 1 July 2015.

IBM would like to thank Seth Hanford and Max Heitman of FIRST for all of their hard work in leading the effort to bring CVSS v3 to the industry.

## Comparison of DNS Kaminsky Bug (CVE-2008-1447)

CVSS scoring from version 2 to version 3



As one of the most important changes in v3, Scope measures whether vulnerability in one software component can impact resources beyond its intended privileges.

*Figure 5. Comparison of DNS Kaminsky Bug (CVE-2008-1447); CVSS scoring from version 2 to version 3*

# About X-Force

## Advanced threats are everywhere. Help minimize your risk with insights from the experts at IBM.

The IBM X-Force research and development team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats.

### IBM Security collaboration

IBM Security represents several brands that provide a broad spectrum of security competency:

- The IBM X-Force research and development team discovers, analyzes, monitors and records a broad range of computer security threats, vulnerabilities, and the latest trends and methods used by attackers. Other groups within IBM use this rich data to develop protection techniques for our customers.
- IBM X-Force Exchange is a robust, global threat-intelligence sharing platform designed to consume, share, and act on threat intelligence—all backed by the scale and reputation of IBM X-Force. Users can search for various threat indicators pulled from machine-generated intelligence, and add context via human intelligence for a collaborative way to research and help stop threats.
- The IBM Security Trusteer® product family delivers a holistic endpoint cybercrime prevention platform that helps protect organizations against financial fraud and data breaches. Hundreds of organizations and tens of millions of end users rely on these products from IBM Security to protect their web applications, computers and mobile devices from online threats (such as advanced malware and phishing attacks).
- The IBM X-Force content security team independently scours and categorizes the web by crawling, independent discoveries, and through the feeds provided by IBM Managed Security Services.
- IBM Managed Security Services is responsible for monitoring exploits related to endpoints, servers (including web servers) and general network infrastructure. This team tracks exploits delivered over the web as well as via other vectors such as email and instant messaging.
- IBM Professional Security Services delivers enterprise-wide security assessment, design and deployment services to help build effective information security solutions.
- IBM QRadar® Security Intelligence Platform offers an integrated solution for security intelligence and event management (SIEM), log management, configuration management, vulnerability assessment and anomaly detection. It provides a unified dashboard and real-time insight into security and compliance risks across people, data, applications and infrastructure.
- IBM Security QRadar Incident Forensics is designed to give enterprise security teams visibility into network activities and clarity around user actions. It can index both metadata and payload content within packet-capture (PCAP) files to fully reconstruct sessions, build digital impressions, highlight suspect content, and facilitate search-driven data explorations aided by visualizations. QRadar Incident Forensics easily integrates with QRadar Security Intelligence Platform and can be accessed using the QRadar one-console management interface.
- IBM Security AppScan® enables organizations to assess the security of web and mobile applications, strengthen application security program management and achieve regulatory compliance by identifying vulnerabilities and generating reports with intelligent fix recommendations to ease remediation. IBM Hosted Application Security Management service is a cloud-based solution for dynamic testing of web applications using AppScan in both pre-production and production environments.
- IBM Security identity and access management solutions help strengthen compliance and reduce risk by protecting and monitoring user access in today's multi-perimeter environments. They help safeguard valuable data and applications with context-based access control, security policy enforcement and business-driven identity governance.

## Contributors

Producing the IBM X-Force Threat Intelligence Quarterly report is a dedicated collaboration across all of IBM. We would like to thank the following individuals for their attention and contribution to the publication of this report.

## For more information

To learn more about IBM X-Force, please visit: **ibm.com**/security/xforce/

| Contributor | Title |
|---|---|
| Brad Sherrill | Manager, IBM X-Force Exchange and X-Force Threat Intelligence Database |
| Doug Franklin | Research Technologist, IBM X-Force Advanced Research |
| Jason Kravitz | Techline Specialist, IBM Security |
| John Kuhn | Senior Threat Researcher, IBM Managed Security Services |
| Leslie Horacek | Manager, IBM X-Force Threat Response |
| Pamela Cobb | WW Market Segment Manager, IBM X-Force and Threat Portfolio |
| Robert Freeman | Manager, IBM X-Force Advanced Research |
| Phil Harrold | Engagement Lead, IBM Emergency Response Services |
| Scott Moore | Software Developer, Team Lead, IBM X-Force Threat Intelligence Database |

[1] Brian Prince, "CryptoWall Ransomware Cost Victims More Than $18 Million Since April 2014: FBI," *SecurityWeek*, 24 June 2015. http://www.securityweek.com/cryptowall-ransomware-cost-victims-more-18-million-april-2014-fbi

[2] Rob Enderle, "Law Enforcement is Powerless Against Cybercriminals: Ransomware and Scams," *IT Business Edge*, 16 April 2015. http://www.itbusinessedge.com/blogs/unfiltered-opinion/law-enforcement-is-powerless-against-cybercriminals-ransomware-and-scams.html

[3] Michael Mimoso, "Ransomware: CryptoWall's Haul: $1M in Six Months," *Threat Post*, 29 August 2014. https://threatpost.com/cryptowalls-haul-1m-in-six-months/107978

[4] High Tech Bridge Security Research, "RansomWeb: emerging website threat that may outshine DDoS, data theft and defacements?" *High Tech Bridge*, 28 January 2015. https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html

[5] "Search Results - web application vulnerabilities," *IBM X-Force Exchange*, Accessed 23 July 2015. https://exchange.xforce.ibmcloud.com/search/web%20application%20vulnerabilities

[6] Jai Vijayan, "'Tox' Offers Ransomware as a Service," *Information Week Dark Reading*, 28 May 2015. http://www.darkreading.com/cloud/tox-offers-ransomware-as-a-service/d/d-id/1320616

[7] "Onion Routing," *Onion Router*, Accessed 23 July 2015. http://www.onion-router.net/Sponsors.html

[8] John Kuhn, "What Surfaces From the Deep, Dark Web," *IBM Security Intelligence Blog*, 17 July 2015. http://securityintelligence.com/what-surfaces-from-the-deep-dark-web/#.Va4DsUbVV4k

[9] "Security Services Research," *IBM Corp.*, Accessed 23 July 2015. http://www-03.ibm.com/security/data-breach/mss-security-threat-research.html

[10] Teri Robinson, "Tor Project, Library Freedom Project, to establish Tor exit nodes in libraries," *SC Magazine*, 31 July 2015. http://www.scmagazine.com/tor-project-library-freedom-project-to-establish-tor-exit-nodes-in-libraries/article/429867/

[11] "Common Vulnerability Scoring System, V3 Development Update," *FIRST*, 10 June 2015. http://www.first.org/cvss

Please Recycle

© Copyright IBM Corporation 2015

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
August 2015

IBM, the IBM logo, ibm.com, AppScan, QRadar, Trusteer, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.