# Security 101 Homework: Security Reporting

## Part I: Symantec

For Part 1 of your homework assignment, you should primarily use the *Symantec Internet Security Threat Report* along with independent research to answer the following questions.

1. What is formjacking?

Formjacking is when cybercriminals inject malicious JavaScript code to hack a website and take over the functionality of the site's form page to collect sensitive user information. Formjacking is designed to steal credit card details and other information from payment forms that can be captured on the checkout pages of websites.

[What is Formjacking and How Does it Work?](https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html)

1. How many websites are compromised each month with formjacking code?

An **average** of 4,800 **websites** a month are **compromised with formjacking** code (Symantec). By stealing only 10 credit cards per website, cyber criminals earn up to $2.2 million through **formjacking** attacks (Symantec)

[**107 Must-Know Data Breach Statistics for 2020**](https://www.varonis.com/blog/data-breach-statistics/)

1. What is Powershell?

**PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language.**

[**PowerShell**](https://en.wikipedia.org/wiki/PowerShell)

1. What was the annual percentage increase in malicious Powershell scripts?  
     
   Use of malicious PowerShell scripts increased by 1,000 percent in 2018, as attackers continued the movement towards living off the land techniques.   
     
   **Malicious PowerShell** attacks **increased** by 661 **percent** from the last half of 2017 to the first half of 2018, and doubled from the first quarter to the second of 2018.

[PowerShell Threats Grow Further and Operate in Plain Sight](https://symantec-blogs.broadcom.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight?om_ext_cid=biz_social_NAM_facebook_Asset%20Type%20%20-%20Blog,Campaign%20-%20Threat%20Alert)

1. What is a coinminer?

What is **CoinMiner** malware? **Coinminers** (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.

[Protection against the Coinminer malware](https://support.norton.com/sp/en/us/home/current/solutions/v125881893)

1. How much can data from a single credit card can be sold for?  **The data from a single credit card can be sold for more than $45, data security provider Symantec reports.**

[**Here's everything a cyber criminal can do if they steal your credit card**](https://www.cnbc.com/2019/09/26/heres-everything-cyber-criminals-can-do-if-they-steal-your-credit-card.html)

1. How did Magecart successfully attack Ticketmaster?

**Magecart** actors breached their systems and, in separate instances, either added to or completely replaced a custom JavaScript module Inbenta made for **Ticketmaster** with their digital skimmer code. ... Many other merchants and providers aside from **Ticketmaster** and Inbenta have been affected by this actor.

[Inside and Beyond Ticketmaster: the Many Breaches of Magecart](https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/)

1. What is one reason why there has been a growth of formjacking?

**Just like any worker, hackers and cybercriminals look for the most efficient way to do their jobs. That's one of the reasons for the recent increase in formjacking, in which credit card data and other personal information is stolen via illicit JavaScript from the forms on e-commerce sites.**

[**Formjacking Attacks Rise in the Retail Sector**](https://biztechmagazine.com/article/2019/04/formjacking-attacks-rise-retail-sector)

1. Cryptojacking dropped by what percentage between January and December 2018?

52 percent

**During 2018**, we blocked more than four times as many **cryptojacking** events as in 2017—almost 69 million **cryptojacking** events in the 12-month **period**, compared to just over 16 million in 2017. However, **cryptojacking** activity did fall **during** the year, **dropping** by 52 **percent between January and December 2018**.

[Internet Security Threat Report Volume 24](https://www.lifelockbusinesssolutions.com/wp-content/uploads/2019/05/ISTR_24_2019_en.pdf) - Page 14

1. If a web page contains a coinmining script, what happens?

If a web page contains a coinmining script, the web page visitors’ computing power will be used to mine for cryptocurrency for as long as the web page is open.

[Cryptojacking: The Hidden Danger to Your Business](https://www.ensighten.com/hubfs/ensighten-website/whitepapers/Cryptojacking-Guide-Ensighten.pdf) - Page 2

1. How does an exploit kit work?

**Exploit kits** are automated threats that utilize compromised websites to divert web traffic, scan for vulnerable browser-based applications, and run malware. **Exploit kits** were developed as a way to automatically and silently **exploit** vulnerabilities on victims' machines while browsing the web.

[**What is an Exploit Kit?**](https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit)

1. What does the criminal group SamSam specialize in?

**Ransomware/Extortion**

This **is** where **SamSam** stands out form the rest. The **group** behind **SamSam** isfocused, which makes its brand of extortion more lethal on the network. **SamSam** isn't commodity ransomware. You **can**'t find it on a **criminal** forum, and it isn't sold as a service.

[SamSam explained: Everything you need to know about this opportunistic group of threat actors](https://www.csoonline.com/article/3263777/samsam-explained-everything-you-need-to-know-about-this-opportunistic-group-of-threat-actors.html)

1. How many SamSam attacks did Symantec find evidence of in 2018?   
   67 different

During **2018**, **Symantec** has to date **found evidence** of **attacks** against 67 different organizations.

[**SamSam: Targeted Ransomware Attacks Continue | Symantec Blogs**](https://symantec-blogs.broadcom.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks)

1. Even though ransomware attacks declined in 2019, what was one dramatic change that occurred?

Year in and year out the increasing adaptivity of offenders has maintained ransomware's position as a major cybersecurity threat. The cybersecurity industry has responded with a similar degree of adaptiveness, but has focussed more upon technical (science) than ‘non-technical’ (social science) factors. This article explores empirically how organisations and investigators have reacted to the shift in the ransomware landscape from scareware and locker attacks to the almost exclusive use of crypto-ransomware. We outline how, for various reasons, victims and investigators struggle to respond effectively to this form of threat. By drawing upon in-depth interviews with victims and law enforcement officers involved in twenty-six crypto-ransomware attacks between 2014 and 2018 and using an inductive content analysis method, we develop a data-driven taxonomy of crypto-ransomware countermeasures. The findings of the research indicate that responses to crypto-ransomware are made more complex by the nuanced relationship between the technical (malware which encrypts) and the human (social engineering which still instigates most infections) aspects of an attack. As a consequence, there is no simple technological ‘silver bullet’ that will wipe out the crypto-ransomware threat. Rather, a multi-layered approach is needed which consists of socio-technical measures, zealous front-line managers and active support from senior management.

[**The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures**](https://www.sciencedirect.com/science/article/pii/S0167404819301336) **The Security Intelligence Report also reveals that hackers have pivoted to more covert means, with an increased focus on exploiting users through social engineering methods like phishing to gain access and exploit data.** [**Phishing rates**](https://www.helpnetsecurity.com/2019/02/28/microsoft-security-intelligence-report-volume-24/) **have increased with cybercriminals also covertly using victims’ compromised computers for cryptocurrency mining.**[**Ransomware and malware attacks decline, attackers adopting covert tactics**](https://www.helpnetsecurity.com/2019/05/20/ransomware-attacks-decline/)

**The report shows that Trojans are currently the biggest malware threat. Attacks involving Trojans are up 650% from the same time last year and attacks increased by 200% in Q1, 2019. The biggest threat is Emotet, which Malwarebytes describes as the “most fearsome and dangerous threat to businesses today.”**

[**Ransomware Attacks Increased by 195% in Q1, 2019 but Trojans Remain the Biggest Threat**](https://www.hipaajournal.com/ransomware-attacks-increased-by-195-in-q1-2019-but-trojans-remain-the-biggest-threat/)

1. In 2018, what was the primary ransomware distribution method?

Email campaigns that use spear phishing and other **methods** to ensnare victims became the **primary method** of **distributing ransomware in 2018**, according to Symantec's ISTR. ... As with most cyber attacks nowadays, **ransomware** assaults typically occur in combination with other attack **techniques**.  
  
[Ransomware Activity Declines, But Remains Dangerous Threat](https://symantec-blogs.broadcom.com/blogs/expert-perspectives/ransomware-activity-declines-remains-dangerous-threat)

1. What operating systems do most types of ransomware attacks still target?  
     
   Windows **is Still** the **Most Targeted System**

Ninety-nine percent of multiple service providers say Windows **operating systems are targeted most** frequently by **ransomware attacks**. However, this doesn't mean that **OS** X, Linux, and Android **are** immune.  
  
[Ransomware Facts, Trends and Statistics for 2020](https://www.safetydetectives.com/blog/ransomware-statistics/)

1. What are “living off the land” attacks? What is the advantage to hackers?   
     
   **What are living off the land attacks**? Any intrusion that involves a malicious attacker deploying a network's own tools against it to extend the **attack** has elements of a LotL approach.  
     
   Advantages:  
   Such attacks are sometimes described as *fileless* or *zero-footprint* attacks as they don't require the installation of malware from an external source. This makes them very difficult for antivirus tools to detect accurately as there are no indicators of outside connections, data exchange or interference.  
     
   [Why 'living off the land' has become a preferred method of cybercrime](https://www.ciodive.com/news/why-living-off-the-land-has-become-a-preferred-method-of-cybercrime/548767/)  
   [Beware of Cyber Attackers “Living off the Land”](https://www.venafi.com/blog/beware-cyber-attackers-living-land)
2. What is an example of a tool that’s used in “living off the land” attacks?  
     
   What tools are used - [Widely used tools](https://www.symantec.com/blogs/feature-stories/its-time-evict-bad-actors-living-land) for ‘Living off the land’ attacks include,

* Mimikatz
* Microsoft’s PS Exec tool
* Windows Management Instrumentation (WMI)
* Windows Secure Copy
* PowerShell scripts
* VB scripts  
    
  Examples of ‘Living off the land’ tactic:

Example 1 - Ransomware Petya/NotPetya outbreak

In June 2018, the [Ransom.Petya](https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931) outbreak hit organizations in Ukraine and other countries leveraging the ‘Living off the land’ tactic.

Petya/NotPetya ransomware used a software supply chain attack as its initial infection vector for compromising the update process of a software accounting program.

* Petya also used system commands during the infection process.
* Once executed, it dropped a recompiled version of LSADump from Mimikatz tool, which is used to steal account credentials from Windows memory.
* The stolen credentials were then used to copy the threat to any computers connected to the network.
* It then launched itself remotely using a dropped instance of PsExec.exe and the Windows Management Instrumentation (WMI) command line tool.

Example 2 - Thrip threat

In 2018, researchers observed cyber espionage campaign dubbed [‘Thrip’](https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets) targeting telecommunication providers, satellites and defense companies by leveraging the ‘Living off the land’ tactic. In the attack campaign, cybercriminals used the Windows utility PsExec to install the Catchamas info-stealer malware.

Example 3 - Separ malware infecting companies via ‘Living off the land’ tactic

Recently, researchers observed a phishing campaign infecting organizations in Southeast Asia, the Middle East, and North America with the [Separ malware](https://www.deepinstinct.com/2019/02/19/a-new-wave-of-the-separ-info-stealer-is-infecting-organizations-through-living-off-the-land-attack-methods/). The malware used a combination of very short scripts or batch files and legitimate executable to evade detection.

* The phishing emails included a malicious PDF attachment that purported to be a self-extracting executable.
* The PDF document disguised as bogus quotations, shipments and equipment specifications.
* Upon opening the malicious PDF attachment, the self-extractor calls wscript.exe to run a Visual Basic Script (VB Script) called adobel.vbs.
* Once the VB Script starts running, it executes an array of short batch scripts which have various malicious functions.

The attack campaign infected almost 200 companies and over 1,000 individuals.  
[Let’s dig deeper on how cybercriminals use ‘Living off the land’ attack tactics](https://cyware.com/news/lets-dig-deeper-on-how-cybercriminals-use-living-off-the-land-attack-tactics-cac5c132)  
  
**Dual-use tools** – hijacking of tools that are used to manage networks and systems which give the attacker the ability to traverse networks, run commands, steal data and even download additional programs or malware. Examples are File Transfer Protocol (FTP) clients or system functions such as PsExec, a Microsoft Sysinternals tool that is used for the execution of processes on other systems.

**Fileless persistence** – a form of attack in which a malicious infection can remain on the system after a reboot even though it wasn't loaded on to the hard disk. This is usually performed by storing malicious scripts in the Windows Registry—such as changes associated with Visual Basic Scripting (VBS).  
  
**Memory only threats** – in which the harmful payload is executed directly in the memory. This is a well-established form of attack; in 2001 the memory only [Code-Red worm](https://www.caida.org/research/security/code-red/) infected a large number of systems through a vulnerability in Microsoft's IIS webserver for example.  
  
**Non-Portable Executable (PE) file attacks** – in this approach the malicious infection affects areas such as JavaScript or PowerShell without using binary executable (EXE) or dynamic-link library (DLL) files.  
  
[Beware of Cyber Attackers “Living off the Land”](https://www.venafi.com/blog/beware-cyber-attackers-living-land)

1. What are zero-day exploits?

A **Zero-day** (also known as **0-day**) vulnerability is a [computer-software](https://en.wikipedia.org/wiki/Computer_software) [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, [hackers](https://en.wikipedia.org/wiki/Hacker) can [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) it to adversely affect computer programs, data, additional computers or a network.[[1]](https://en.wikipedia.org/wiki/Zero-day_(computing)#cite_note-1) An exploit directed at a zero-day is called a **zero-day exploit,** or **zero-day attack.**[**Zero-day (computing)**](https://en.wikipedia.org/wiki/Zero-day_(computing))

1. By what percentage did zero-day exploits decline in 2018?

The use of zero-day exploits continued to decline last year, with only 23% of attack groups using zero-days. Some attack groups such as [**Gallmaker**](https://www.securityweek.com/cyberspy-group-gallmaker-targets-military-government-organizations) switched to relying solely on “living off the land” techniques, without using malicious code.

[Supply Chain Attacks Nearly Doubled in 2018: Symantec](https://www.securityweek.com/supply-chain-attacks-nearly-doubled-2018-symantec)

1. What are two techniques that worms such as Emotet and Qakbot use?  
     
   **Social Engineering, Brute Force, & Living-off-the-land**  
     
   How does Emotet spread?

The primary distribution method for Emotet is through malspam. Emotet ransacks your contacts list and sends itself to your friends, family, coworkers and clients. Since these emails are coming from your hijacked email account, the emails look less like spam and the recipients, feeling safe, are more inclined to click bad URLs and download infected files.

If a connected network is present, Emotet spreads using a list of common passwords, guessing its way onto other connected systems in a [brute-force ­attack](https://en.wikipedia.org/wiki/Brute-force_attack). If the password to the all-important human resources server is simply “password” then it’s likely Emotet will find its way there.

Researchers initially thought Emotet also spread using the [EternalBlue/DoublePulsar vulnerabilities](https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/), which were responsible for the [WannaCry and NotPetya attacks](https://blog.malwarebytes.com/threat-analysis/malware-threat-analysis/2017/07/all-this-eternalpetya-stuff-makes-me-wannacry/). We know now that this isn't the case. What led researchers to this conclusion was the fact that [TrickBot](https://blog.malwarebytes.com/101/2018/11/trickbot-takes-top-business-threat/), a Trojan often spread by Emotet, makes use of the EternalBlue [exploit](https://www.malwarebytes.com/exploits/) to spread itself across a given network. It was TrickBot, not Emotet, taking advantage of the EternalBlue/DoublePulsar vulnerabilities.  
  
**Qakbot**

Since February 2018, Emotet has been used to spread [W32.Qakbot](https://www.symantec.com/security-center/writeup/2009-050707-0639-99), a family of banking Trojans known for behaving like network worms.

Like Emotet, Qakbot can self-propagate. Qakbot attempts brute force access to spread across networks and also uses “[living-off-the-land](https://www.symantec.com/connect/blogs/attackers-are-increasingly-living-land)” tools to propagate. It uses PowerShell to download and run Mimikatz ([Hacktool.Mimikatz](https://www.symantec.com/security-center/writeup/2012-042615-3731-99)), an open-source credential stealing tool that allows attackers to move rapidly across a network once they have established an initial foothold.

The fact that both Emotet and Qakbot have self-spreading capabilities mean that once these threats get onto your network they can spread aggressively. The fact that both attempt brute force access to spread across networks also increases the risk of users being locked out of their devices. A spike in Qakbot detections in February 2018 indicates that “double-spreading” of the threat was taking place, meaning that Mealybug was using Emotet to spread Qakbot across networks, while Qakbot was simultaneously using its own self-spreading capabilities. The account lockout scenario is a very real danger, and a potential major headache for organizations.  
  
[The Evolution of Emotet: From Banking Trojan to Threat Distributor](https://symantec-blogs.broadcom.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor)

1. What are supply chain attacks? By how much did they increase in 2018?

**The number of supply chain attacks observed last year was 78% higher compared to the previous year, a new Symantec report reveals.**

[Supply Chain Attacks Nearly Doubled in 2018: Symantec](https://www.securityweek.com/supply-chain-attacks-nearly-doubled-2018-symantec)

1. What challenge do supply chain attacks and living off the land attacks highlight for organizations?

Both **supply chain** and **living**-**off-the-land attacks highlight** the **challenges** facing **organizations** and individuals, with **attacks** increasingly arriving through trusted channels, using fileless **attack** methods or legitimate tools for malicious purposes.

[nevada office of cyber defense coordination](https://dps.nv.gov/uploadedFiles/dpsnvgov/content/divisions/OCDC/home/OCDC_Annual%20Report_2019.pdf) - Page 8

1. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?

**The 20 most active groups tracked by Symantec targeted** an **average** of 55 **organizations** over the past three years.

[Internet Security Threat Report Volume 24](https://www.lifelockbusinesssolutions.com/wp-content/uploads/2019/05/ISTR_24_2019_en.pdf) - Page 52

1. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?

ESPIONAGE INDICTMENTS BY U.S. AUTHORITIES :49

CHINA - 19

RUSSIA - 18

IRAN - 11

NORTH KOREA - 1  
  
Source: Page 49 of the provided Symantec\_Report.pdf (Facts and Figures)

1. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
     
   One of the most **common** network **attacks** occurs by exploiting the limitations of the commonly used network protocols Internet Protocol (IP), Transmission Control Protocol (TCP) or Domain Name System (DNS)  
     
   [A survey of emerging threats in cybersecurity](https://www.sciencedirect.com/science/article/pii/S0022000014000178)
2. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
     
   A more insidious threat to the cloud emerged in 2018 with the revelation of several vulnerabilities in hardware chips. Meltdown and Spectre exploit vulnerabilities in a process known as speculative execution. Successful exploitation provides access to memory locations that are normally

Forbidden. This is particularly problematic for cloud services because while cloud instances have their own virtual processors, they share pools of memory—meaning that a successful attack on a single physical system could

result in data being leaked from several cloud instances.

Source: Page 19 of the provided Symantec\_Report.pdf (Year-In-Review)

1. What are two examples of the above cloud attack?   
     
   Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks

A DoS/DDoS attack renders a website unavailable to users, but a successful one will hit an entire online user database. In a DoS attack, a perpetrator can use a single Internet connection to exploit a software vulnerability or flood the target with fake requests and finally cause that the site is made unavailable and prevent it from responding to requests from the legitimate users.  
  
Insider attacks

Insider attacks remain one of the top threats for various organizations, even if you don't use cloud infrastructure. While most employees are trustworthy, it's always a good idea to have a clear understanding of who has access to certain files and documents. Every organization should have multi-layered security policies in place, meaning that employees should have access only to those documents that are directly related to their everyday work.

It's actually easy to implement such policies, but people often overlook them

[Cloud Attack Vectors and Counter Measures](https://www.globaldots.com/blog/cloud-attack-vectors)

1. Regarding Internet of Things (IoT) attacks, what were the two most common infected devices and what percentage of IoT attacks were attributed to them?   
     
   **75% of infected devices in IoT attacks are routers and connected cameras**[Symantec data](https://www.symantec.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse) indicates that infected routers accounted for 75% of IoTattacks in 2018, and connected cameras accounted for 15% of them.

[20 Surprising IoT Statistics You Don't Already Know](https://securityboulevard.com/2019/09/20-surprising-iot-statistics-you-dont-already-know/)  
  
The overall volume of IoT attacks remained high in 2018

and consistent (-0.2 percent) compared to 2017. Routers

and connected cameras were the most infected devices and

accounted for 75 and 15 percent of the attacks respectively.

It’s unsurprising that routers were the most targeted devices

given their accessibility from the internet. They’re also

attractive as they provide an effective jumping-off point

for attackers.

Source: Page 20 of the provided Symantec\_Report.pdf (Year-In-Review)

1. What is the Mirai worm and what does it do?   
     
   **Mirai** (Japanese: 未来, lit. 'future') is a malware that turns networked devices running Linux into remotely controlled bots that **can** be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.  
   [Mirai (malware)](https://en.wikipedia.org/wiki/Mirai_(malware))
2. Why was Mirai the third most common IoT threat in 2018?   
   **The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16 percent of the attacks, was the third most common IoT threat in 2018. Mirai is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection, as devices often remain unpatched. The worm also expanded its target scope by going after unpatched Linux servers. Another noticeable trend was the increase in attacks against industrial control systems (ICS). The Thrip group went after satellites, and Triton attacked industrial safety systems, leaving them vulnerable to sabotage or extortion attacks. Any computing device is a potential target.**   
     
   Source: Page 20 of the provided Symantec\_Report.pdf (Year-In-Review)
3. What was unique about VPNFilter with regards to IoT threats?  
   **The emergence of VPNFilter in 2018 represented an evolution of IoT threats. VPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove. With an array of potent payloads at its disposal, such as man in the middle (MitM) attacks, data exfiltration, credential theft, and interception of SCADA communications, VPNFilter was a departure from traditional IoT threat activity such as DDoS and coin mining. It also includes a destructive capability which can “brick,” or wipe a device at the attackers’ command, should they wish to destroy evidence. VPNFilter is the work of a skilled and well-resourced threat actor and demonstrates how IoT devices are now facing attack from many fronts.**

Source: Page 20 of the provided Symantec\_Report.pdf (Year-In-Review)

1. What type of attack targeted the Democratic National Committee in 2019?   
   **Then, in January 2019, the DNC revealed it was targeted by an unsuccessful spear-phishing attack shortly after the midterms had ended. The cyber espionage group APT29, which has been attributed by the U.S. Department of Homeland Security (DHS) and the FBI to Russia, is thought to be responsible for the campaign.**

Source: Page 21 of the provided Symantec\_Report.pdf (Year-In-Review)

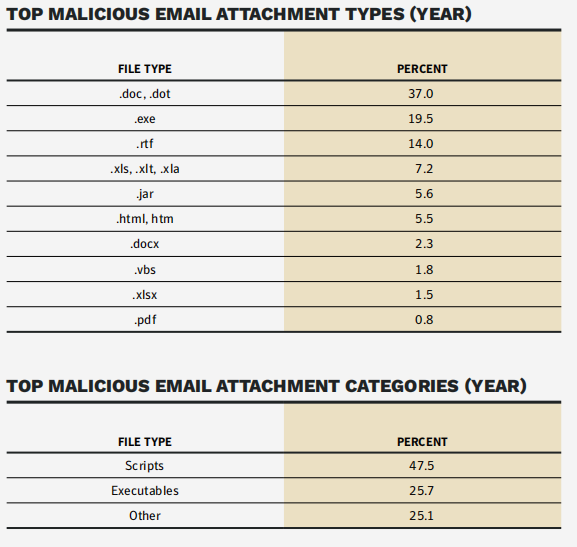
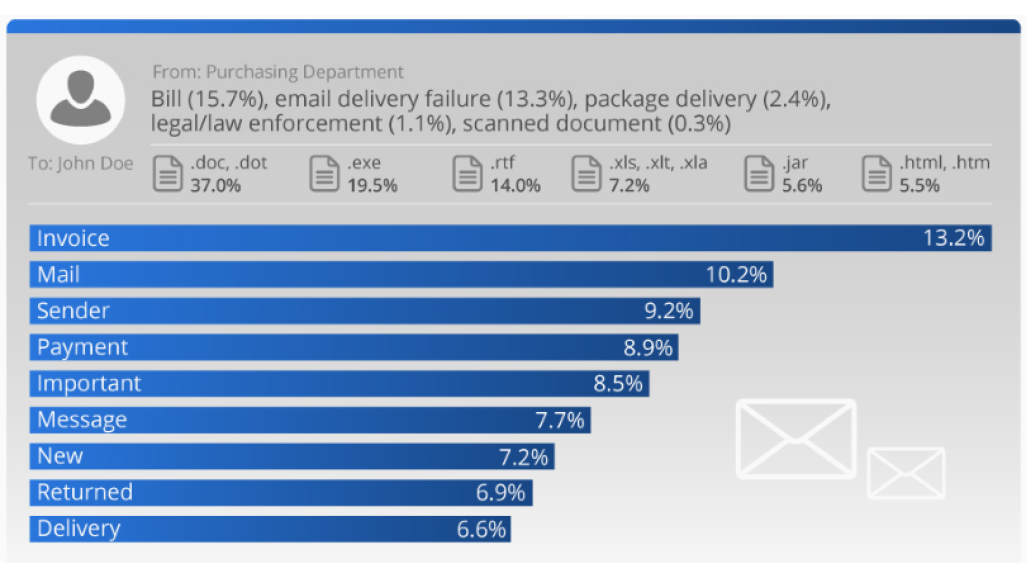
1. What were 48% of malicious email attachments in 2018?   
   Symantec says that 48 percent of the malicious email attachments going out in 2018 were Office files of some sort, and that's way up from 5 percent in 2017.  
   ['Invoice' in Your Email? Office File Attached? Beware!](https://www.pcmag.com/news/invoice-in-your-email-office-file-attached-beware)

1. What were the top two malicious email themes in 2018?

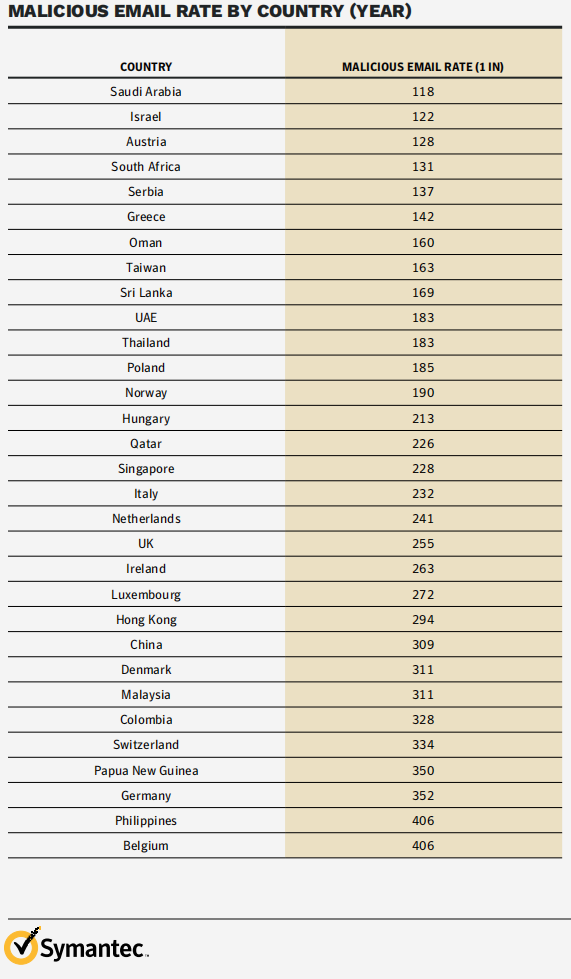
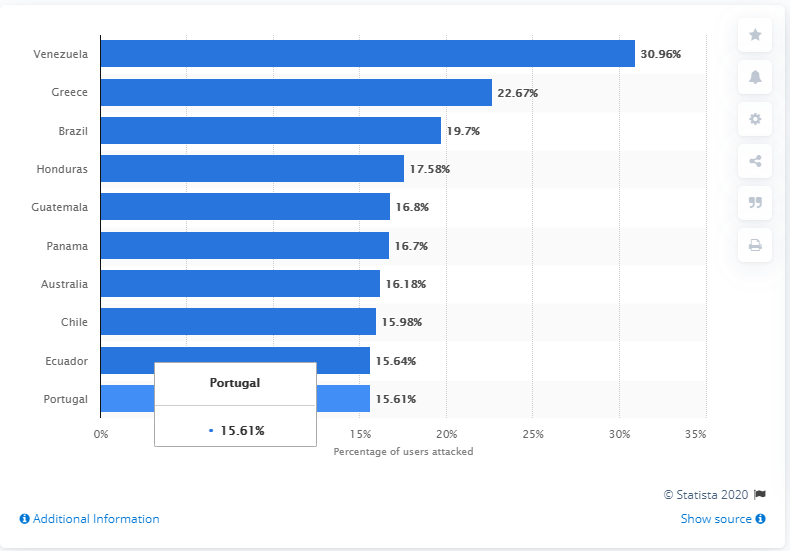
|  |  |  |
| --- | --- | --- |
| **Rank** | **Phishing Subject/Theme** | **Number of Reported Emails** |

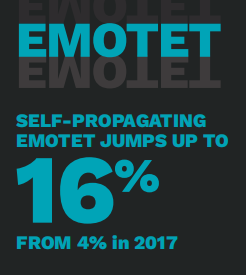
|  |  |  |
| --- | --- | --- |
| 1  2 | Attached Invoice  Payment Notification | 4,796  2,267 |

[What are the Top Phishing Lures of 2018?](https://www.spamtitan.com/blog/top-phishing-lures-of-2018/)

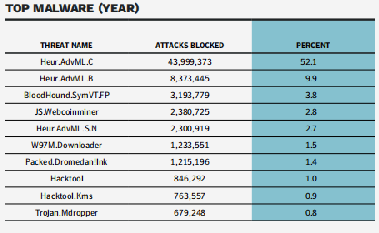
1. What was the top malicious email attachment type in 2018?   
     
     
     
     
   “One thing that should always arouse suspicion is an attachment you weren't expecting. In particular, you should be on the lookout for just five types of files. According to analysis [by Helsinki-based security provider F-Secure](https://press.f-secure.com/2018/07/31/spam-is-still-the-choice-of-online-criminals-40-years-later/) 85% of all malicious emails have a .DOC, .XLS, .PDF, .ZIP, or .7Z attached.”  
     
   [These Are The Five Most Dangerous Email Attachments](https://www.forbes.com/sites/leemathews/2018/08/01/these-are-the-five-most-dangerous-email-attachments/#2ace89b12d1b)  
     
   

['Invoice' in Your Email? Office File Attached? Beware!](https://www.pcmag.com/news/invoice-in-your-email-office-file-attached-beware)

1. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
     
     
     
   The United States is once again, and for the foreseeable future, the most targeted country by threat actors’ phishing attacks. Making up an astonishing 84% of all phishing volume, the U.S. saw a single percent decline from 85% last year.  
   [These Are the Top Most Targeted Countries by Phishing Attacks](https://info.phishlabs.com/blog/top-targeted-countries-by-phishing-attacks-2019) ****[**• Phishing: distribution of attacks by country 2019**](https://www.statista.com/statistics/266362/phishing-attacks-country/)
2. What is Emotet and how much did it jump in 2018?   
   [**Emotet**](https://en.wikipedia.org/wiki/Emotet) is a [malware](https://en.wikipedia.org/wiki/Malware) strain and a [cybercrime](https://en.wikipedia.org/wiki/Cybercrime) operation. The malware, also known as **Geodo** and **Mealybug**, was first detected in 2014 and remains active, deemed one of the most prevalent threats of 2019.



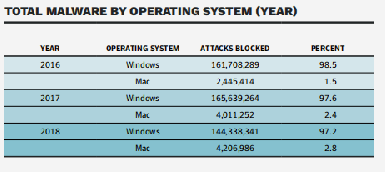
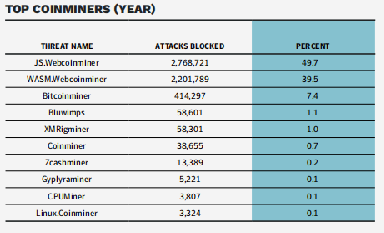
Emotet continued to aggressively expand its market share in 2018, accounting for 16 percent of financial Trojans, up from 4 percent in 2017.   
  
Emotet was also being used to spread Qakbot, which was in 7th place in the financial Trojans list, accounting for 1.8 percent of detections.Both of these threats present further serious challenges for organizations due to their self-propagating functionality  
Source: Page 21 of the provided Symantec\_Report.pdf (Facts and Figures)

1. What was the top malware threat of the year? How many of those attacks were blocked?  
     
   “What’s the worst malware so far into 2018? The [worst botnets and banking trojans, according to Webroot](https://community.webroot.com/t5/Announcements/Nastiest-Malware-2018/td-p/332217), were Emotet, Trickbot, and Zeus Panda. Crysis/Dharma, GandCrab, and SamSam were the worst among ransomware. The top three in cryptomining/cryptojacking were GhostMiner, Wanna Mine, and Coinhive.”  
   [Worst malware and threat actors of 2018 so far](https://www.csoonline.com/article/3319116/worst-malware-and-threat-actors-of-2018-so-far.html) **PROTECTION AGAINST MALWARE**

**As technically feasible, deploy anti-malware software on all endpoints capable of running anti-malware software including, but not limited to: laptops, desktops, servers, tablets, and smartphones.**

* **Configure anti-malware software to perform periodic scans of the endpoint and real-time scans of all files from external sources as the files are downloaded, opened, or executed;**
* **Configure anti-malware software to quarantine any malicious code detected and to send an alert to the organization’s IT service desk and/or information security team;**
* **Configure anti-malware software to automatically apply and keep current with anti-malware vendor updates;**
* **Ensure anti-malware mechanisms are actively running and cannot be disabled or altered by users; and**
* **Configure anti-malware software to maintain an audit log of all anti-malware software activity.**

[**Mitigating the Risk of Malware Infections**](https://www.cyber.nj.gov/be-sure-to-secure/mitigating-the-risk-of-malware-infections)

1. Malware primarily attacks which type of operating system?   
   Different **types** of **malware** include viruses, **spyware**, ransomware, and **Trojan** horses. **Malware attacks** can occur on all sorts of devices and **operating systems**, including Microsoft Windows, macOS, Android, and iOS.  
   [Malware attacks: What you need to know](https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html) ****
2. What was the top coinminer of 2018 and how many of those attacks were blocked?   
     
   **Disable JavaScript on specific sites**

If you suspect a website is using your computer to mine cryptocurrencies without your permission, you can simply block JavaScript altogether.

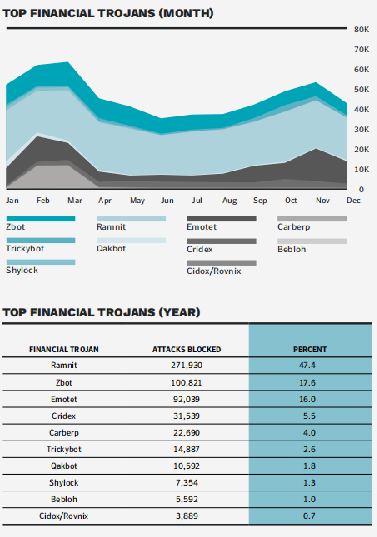
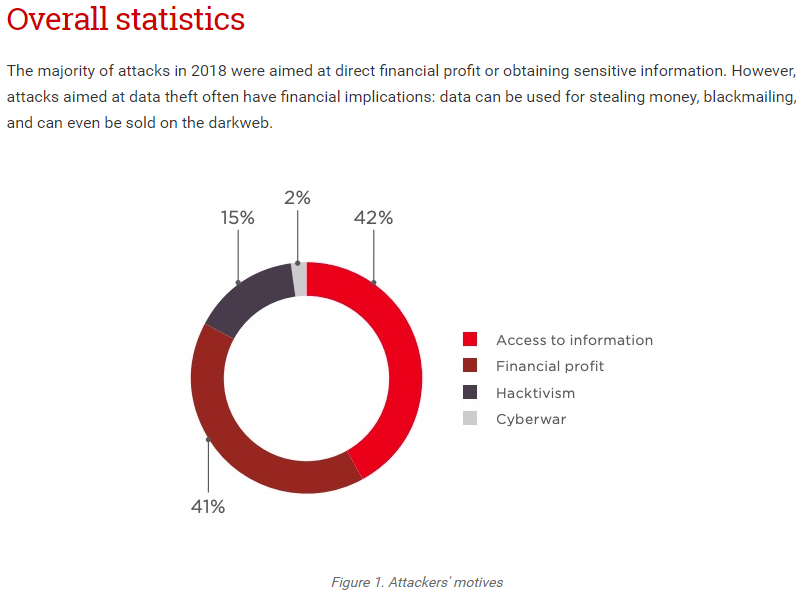
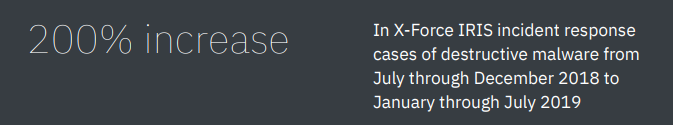
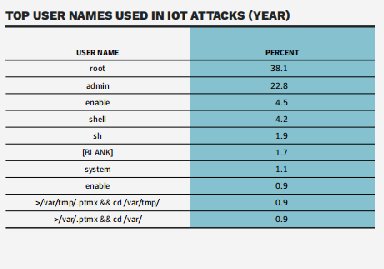
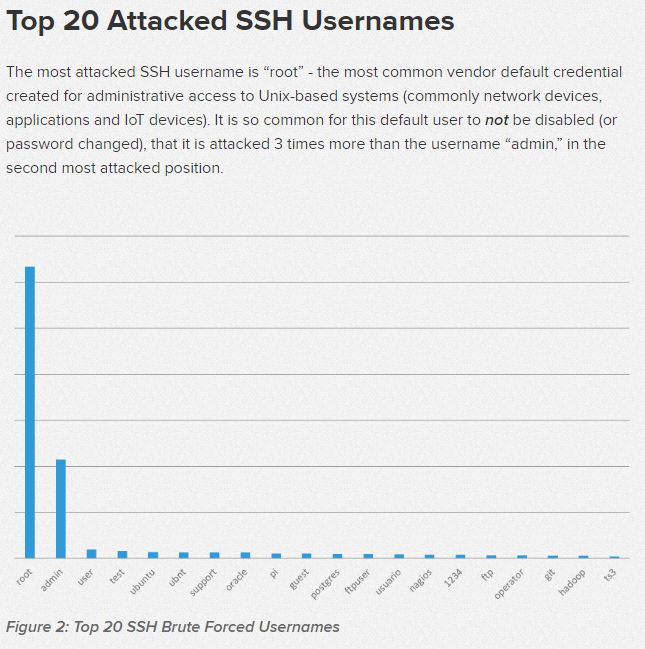
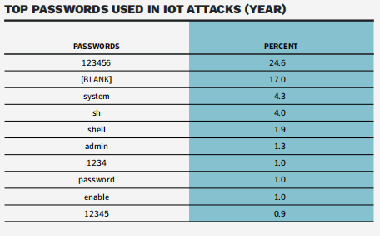
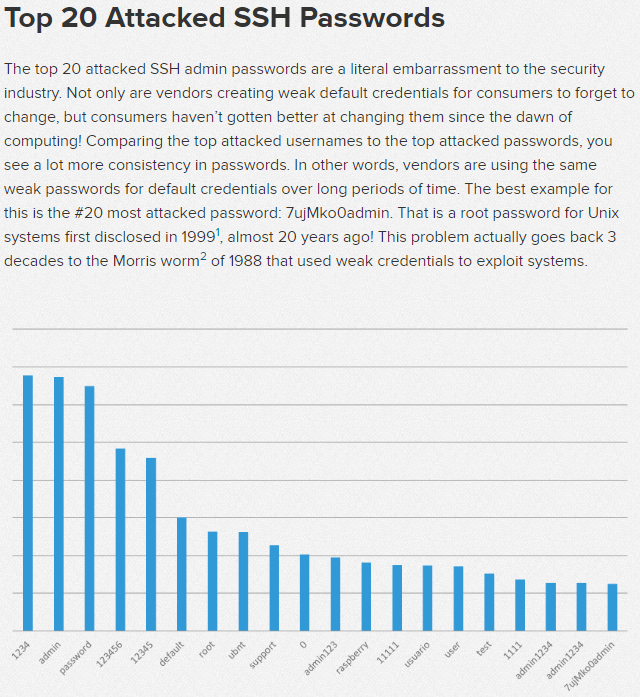
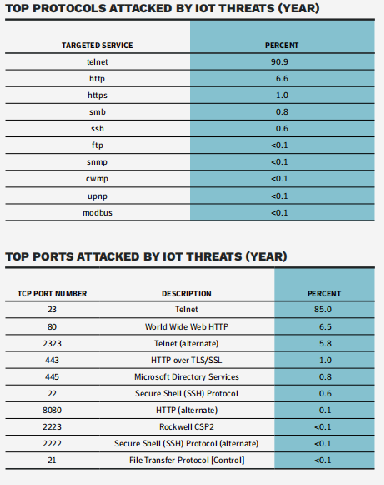
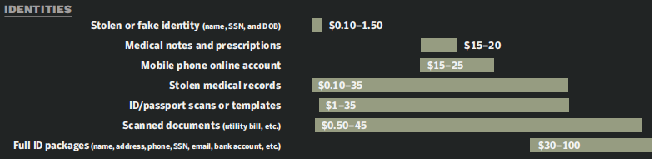
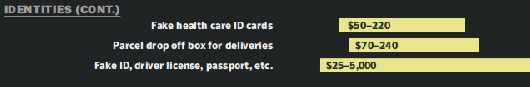
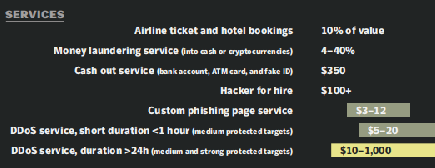
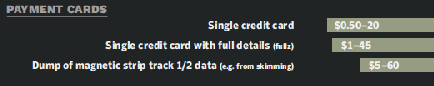
The problem, however, is that this is a very aggressive way to block mining and will break many websites. Facebook, for instance, will not load without JavaScript enabled.

### **Coin mining blockers**

If you don't want to use an ad blocker or just want to specifically block coin mining, there are a handful of extensions available

* No Coin ([Chrome](https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl?utm_source=chrome-ntp-icon), [Firefox](https://addons.mozilla.org/en-US/firefox/addon/no-coin/), [Opera](https://addons.opera.com/en/extensions/details/no-coin/?display=en))
* minerBlock ([Chrome](https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl?utm_source=chrome-ntp-icon), [Firefox](https://addons.mozilla.org/en-US/firefox/addon/minerblock-origin/), [Opera](https://addons.opera.com/en/extensions/details/minerblock/?display=en))
* Anti Miner ([Chrome](https://chrome.google.com/webstore/detail/anti-miner-no-1-coin-mine/ibhpgkhoicjhklmbhdoeikeggbeejonj?utm_source=chrome-ntp-icon))
* Coin-Hive Blocker ([Chrome](https://chrome.google.com/webstore/detail/coin-hive-blocker/ccagdbjcbhmcdcbbknfebhhdbolnfimo?hl=en))

These extensions work by blacklisting known domains and mining scripts. They're regularly updated and are among the best hands-off approaches to block mining. On the flip side, if you want to support a website by allowing it to mine, you can whitelist it.   
[How to stop websites from using your computer to mine Bitcoin (and more)](https://www.cnet.com/how-to/how-to-stop-sites-from-using-your-cpu-to-mine-coins/)

1. What were the top three financial Trojans of 2018?   
   Trickbot, Gozi, Ramnit, and IcedID **were** the most active banking **Trojans** in **2018**, and while other forms of malware have grown in popularity, it **is** the most active -- and prevalent -- forms of **financial** malware **which are** now being spread through cybercriminal partnerships  
   [Bank hackers team up to spread financial Trojans worldwide](https://www.zdnet.com/article/bank-hackers-team-up-to-spread-financial-trojans-worldwide/)  
   
2. What was the most common avenue of attack in 2018?   
     
   [Cyber Security Threat Trends 2018 and Forecasts for 2019: Attack Statistics and Facts](https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018/)
3. What is destructive malware? By what percent did these attacks increase in 2018?   
   **Destructive malware** is malicious software with the capability to render affected systems inoperable and challenge reconstitution. Most **destructive malware** variants cause destruction through the deletion, or wiping, of files that are critical to the operating system's ability to run.  
     
     
     
   [What is destructive malware?](https://www.ibm.com/downloads/cas/XZGZLRVD)
4. What was the top user name used in IoT attacks?   
     
     
     
   [Spaceballs Security: The Top Attacked Usernames and Passwords](https://www.f5.com/labs/articles/threat-intelligence/spaceballs-security--the-top-attacked-usernames-and-passwords)
5. What was the top password used in IoT attacks?   
     
     
   [Spaceballs Security: The Top Attacked Usernames and Passwords](https://www.f5.com/labs/articles/threat-intelligence/spaceballs-security--the-top-attacked-usernames-and-passwords)
6. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
     
   
7. In the underground economy, how much can someone get for the following?
   1. Stolen or fake identity:  
      
   2. Stolen medical records:  
      
   3. Hacker for hire:  
      
   4. Single credit card with full details:  
      
   5. 500 social media followers:  
      