ManageEngine
Log360

Combating hacking techniques: **How to defend against DDoS, ransomware, and cryptojacking**

www.manageengine.com/log360

Table of Contents

From the authors

Hi there. Thanks for downloading this e-book.

The COVID-19 pandemic has dealt both individuals and businesses a major blow. We've all been left vulnerable to something that we can't see but has a destructive effect on our lives and livelihoods.

While healthcare professionals are in the direct line of fire, the fight against this pandemic is a collective effort. This is because of the ripple effect the pandemic has.

We're not only battling a biological threat but also a rise in digital threats. Hackers around the world are leveraging the uncertainty around the pandemic and the loopholes in the sudden shift to remote work to launch various attacks. Numerous organizations around the globe have already fallen victim to cyberattacks and have suffered disruptions in business operations.

Take a look at some of these worrying stats:

- Q1 of 2020 has seen a 542% jump of distributed denial-of-service (DDoS) attacks when compared to Q4 of 2019.[1]
- According to the Threat Landscape Trends report for Q2 2020, by US cyber-security vendor Symantec, cryptojacking saw a 163% increase in detections, compared to previous quarters.[2]
- According to a survey by NinjaRMM, 35% of organizations indicate that ransomware attacks resulted in up to $5 million in damages.[3]

In a crisis like this, organizations have to take the necessary measures to protect against security breaches.

We created this e-book to educate and create awareness about the security threats and major cyberattacks that are plaguing businesses right now. Our objective is to dissect three popular attacks - DDoS, cryptojacking and ransomware - and provide tips on ramping up your organization's security defenses. After reading this e-book, you should also have a clear idea about the threats these three attacks can cause to your business.

The digitization of services has paved the way for easy accessibility at fast speeds for users all over the globe. While this has no doubt brought about many advantages, it has also increased the number of vulnerabilities and the attack surface.

Not only are cyber threats growing more potent, the ways in which attacks take place are also evolving. Attackers have specific goals when attacking your systems. They can paralyze your systems, steal sensitive data, lock your files, and disrupt overall operations of your business. Organizations should therefore place heavy emphasis on cyber-resilience.

> *Threat is a mirror of security gaps. Cyber-threat is mainly the reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience.*[4]
>
> Stephane Nappo, Global CISO of 2018

Cyberattacks happen for a variety of reasons. Attacks in recent times have occurred due to political motivation, attempts to eliminate competition, unhappy insiders, and corporate espionage.

With so much at stake, organizations have to formulate a framework of cybersecurity strategies that can adapt to new and evolving threats. Cybersecurity involves not just technological defenses but a comprehensive process that keeps employees updated about security policies, ensures there's a thorough evaluation of loopholes, and formulates incident response and threat mitigation plans.

This e-book will walk you through the common vulnerabilities that exist in organizations' networks and how hackers exploit them. Although this book is written with the pandemic in mind, the information here is relevant to any scenario. This e-book also covers mitigation strategies you can use against DDoS, cryptojacking and ransomware with ManageEngine Log360.

Chapter 1: Distributed denial of service (DDoS) - When your server freezes up

On July 22, 1999, the world saw the birth of a new cyberattack that soon snowballed into a widespread commercialized phenomenon that we know as DDoS. The University of Minnesota's server was the first known victim of a DDoS attack. The malicious script that identified itself at Trin00 corrupted many computers, turning them into a robot army. This army began sending multiple requests to the university's server, clogging up the queue and preventing the server from servicing legitimate requests.

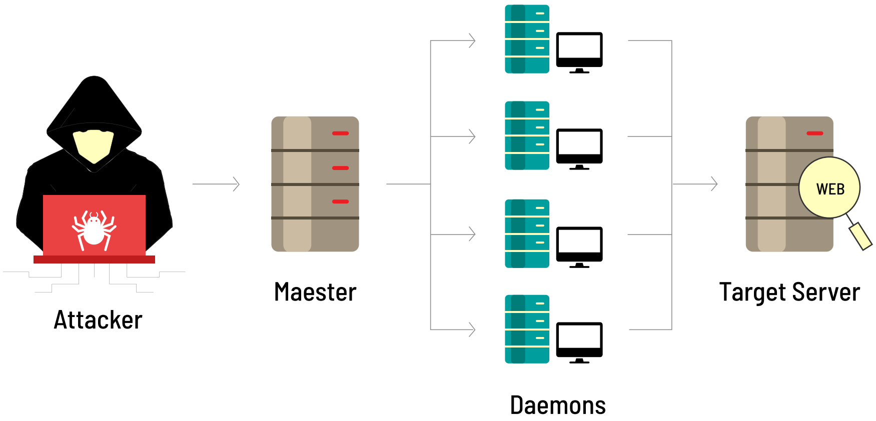
How DDoS attackers trespass on your network

Years after the first attack, DDoS is still a popular attack method, and affects university and government networks frequently.

We will now discuss the different stages of a DDoS attack.

Stage 1: Infiltration of an organization's network

The first stage of the attack begins when a computer gets infected with malicious software that is designed to spread across the network. The malware gets delivered to the computer through a phishing email or gets downloaded when the user visits a malicious website. This particular computer, in DDoS terms, is referred to as the master. This master computer goes on to recruit subordinate computers (daemons) to its rogue army by spreading the malware to them as well. These daemon computers are the ones that actually conduct the attack.



How DDoS targets a server

Stage 2: Overwhelming a target's servers

The master computer sends a command to the daemons with the IP address of the target server. Hackers could leverage the Internet Relay Chat (IRC) protocol along with previously configured IRC servers and channels to control the daemons remotely.

The daemons begin sending phony requests to the target server at a high speed, quickly overloading it. When the target server is overwhelmed with requests, it can't differentiate between authentic requests and phony ones. It freezes and can't process any legitimate requests for the duration of the attack.

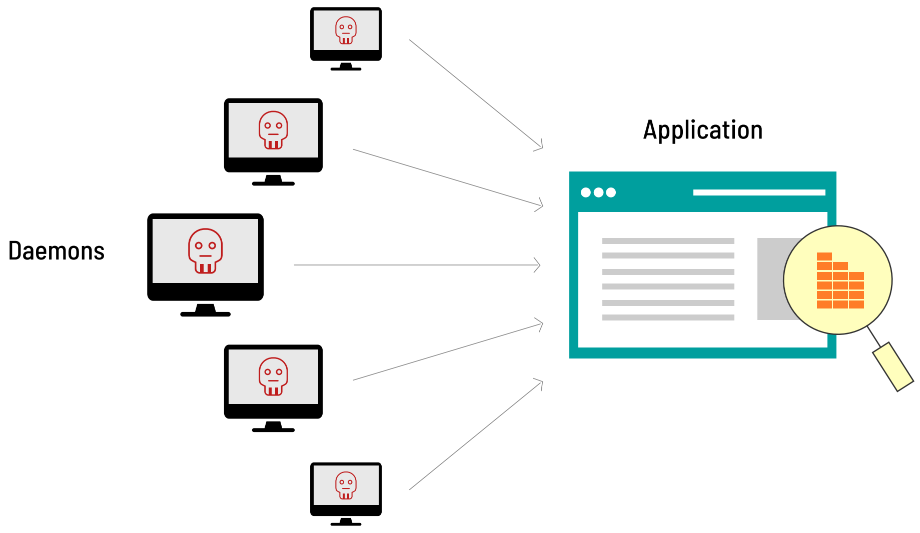
Hackers use tactics like IP spoofing — a technique that masks the IP address of the hacker controlling the masters and daemons -- to makes it hard for administrators to track down the IP addresses of the master and daemons.

The physiology of a DDoS attack

There are three main types of DDoS attacks. These are i) Application layer attacks ii) Volume-based attacks, and iii) Protocol-based attacks.[5]

Application layer attacks In this type of attack, hackers target specific applications and overwhelm them with fraudulent requests. The goal of the attack is to restrict legitimate users from using the application. Hackers do this by mimicking the behavior of legitimate users.

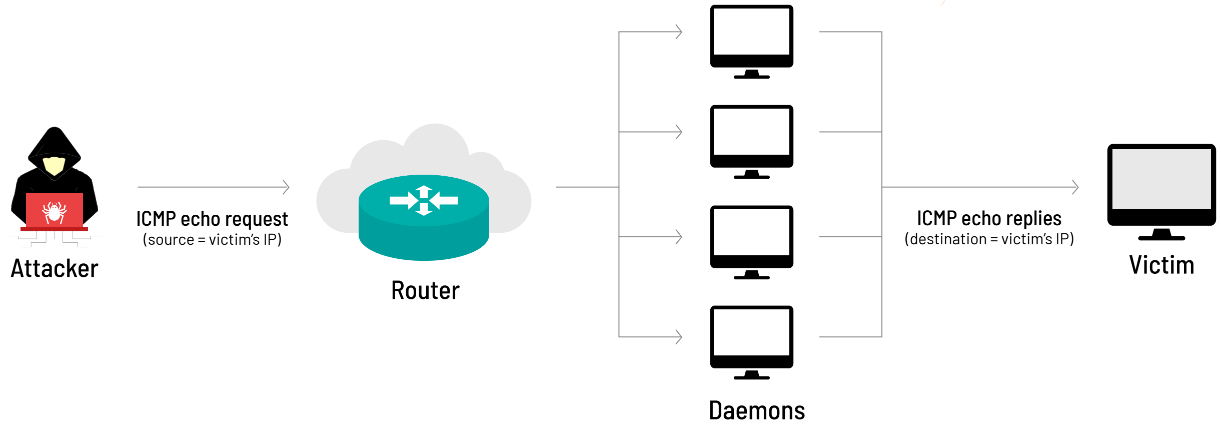
Some of the common application attacks are Layer 7 HTTP flooding and DNS server targeted attacks. IoT devices are also susceptible to an application layer attack. The magnitude of an application layer attack is measured by requests per second (RPS).



The attacker sends numerous fraudulent requests which leads to flooding

Volume-based attacks This type of attack preys on CPU bandwidth by inducing a high volume of traffic. This slows down the resources and prevents users from acclayeressing services. It starts with the creation of a botnet: a group of infected computers that conducts the attack.

The requests from the botnet may seem legitimate at first before they multiply in volume and start to suppress genuine requests. Apart from flooding the target server with phony requests, a volume-based DDoS attack may also disrupt communication between computers by targeting the routers in the network. The magnitude of volume-based attacks are measured in bits per second (bps).



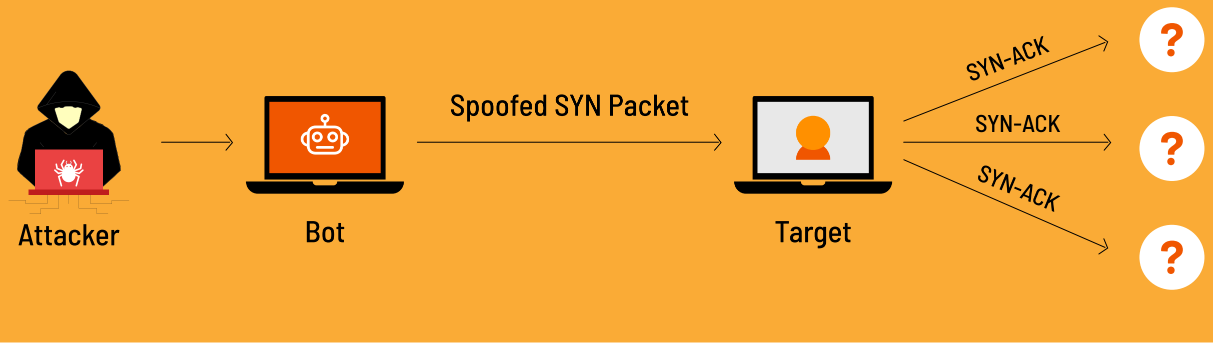
Target device is flooded with ICMP echo-request packets, forcing the network to respond with an equal number of reply packets, resulting in a denial of service to legitimate traffic.

Protocol-based attacks DDoS attacks based on protocols exploit weaknesses in Layers 3 and 4 protocols. Measured in packets per second (pps), this type of attack preys on the server's resources or other network hardware while a request is being processed. These attacks try to overload your network by sending either more packets than your server can handle or using more bandwidth than your network ports can handle. This results in a disruption of services.

In an attack of this type, attackers target intermediate communication equipment such as firewalls to overwhelm server resources. It can exhaust these resources, leading to a disruption of service.

An example of a protocol-based attack

SYN-ACK flood is a protocol-based attack method where the attacker sends a target server spoofed SYN-ACK packet at a high rate. A server requires significant processing power to understand why it is receiving such packets out of order (the usual order being: SYN, SYN-ACK, ACK TCP three-way handshake mechanism). This can lead to a busy server unable to handle legitimate traffic.



Motivations behind a DDoS attack

So, what's in it for hackers? How do they benefit from clogging up your servers and stopping your business operations? Here are some of the reasons behind DDoS attacks.

Targeting a competitor

Organizations have been known to hire hackers to carry out a DDoS attack on their competitors. This malicious act can be lucrative for the company that organized the attack, because while their competitors are busy dealing with the attack, the company that planned the attack can increase their customer base.

Hacktivism

Hackers have made political statements in the past by launching DDoS attacks on government websites. These attacks have allowed hackers to gain celebrity status to spread a message or show some form of protest.

Demanding a ransom

Criminals realized that there was a lot of money to be made from demanding a ransom from an organization that was desperate to resume its halted operations. Hackers have been known to warn potential victims about an impending DDoS attack to extort bitcoin payments out of them.

Boredom

Believe it or not, boredom is also one of the common reasons behind DDoS attacks.

Chapter 2: DDoS in the era of COVID-19

Since the pandemic was declared, people have taken to working from home. While this ensures business continuity, it has also created fertile grounds for DDoS attacks to take place.

Kaspersky's Q1 2020 report on DDoS attacks depicts a "significant increase in the quantity and quality of DDoS attacks."[6] The number of DDoS attacks went up by 80% in the first quarter of 2020 as compared to Q1 2019.[7] The focus of DDoS hackers is on educational institutions, medical facilities, and government websites.[8]

There have been four significant DDoS attacks since the start of the pandemic.[9] These are:

1. Attack on the U.S Department of Health and Human Services

The department's website was earning a lot of traffic from users who wanted to know important information regarding the virus. DDoS attackers created spoof requests and tried overloading the servers, depriving users access to critical information. On top of that, attackers spread false information about a nationwide quarantine via emails and social media. Fortunately though, the attack wasn't enough to collapse the servers, and the website continued to function.

2. Attack on a French group of hospitals

A Paris-based group of hospitals, Assistance Publique-Hôpitaux de Paris, faced interference with its medical facilty's network infrastructure. This resulted in hospital workers being unable to access emails and applications on the network.

3. Attacks on essential service websites in Greece

Government websites hosting important information about essential services found themselves the target of malicious DDoS attacks. Information regarding fire services and police services were removed from the site.

4. Attack on cryptocurrency exchanges

Cryptocurrency exchanges OKEx and Bitfinex were victims of DDoS attacks. OKEx first noticed its servers were dealing with increased output. The attack lasted two days with incoming traffic ranging between 200GB to 400GB per second. However, the systems weren't crippled by the attack. A few days later both Bitfinex and OKEx experienced another wave of DDoS attacks, this time interrupting all trading activities.

Chapter 3: DDoS trends in 2020 and beyond

The year 2020 has witnessed a sharp rise in the number of DDoS-related cyberattacks. Therefore businesses need to be updated about the major cyber threat trends that they are up against. This will help them improve their security posture.

Here are six major cyber threat trends for 2020 and beyond that organizations should prepare for.[10]

Trend 1: The NXNSAttack

One of the biggest DDoS threats to the security of your business is the NXNSAttack. The NXNSAttack is not new and first came to light in 2016 when DYN servers, one of the titans providing the DNS services, were attacked by a botnet called Mirai.[11] This attack was already known to take down industry Goliaths around the globe.

What's an NXNS attack, and why it is so dangerous?

Unlike protocol-based, volume-based, or application-based DDoS attacks that directly target the victim's servers with a flood of requests, this attack focuses on the name resolution capability of the victim. This attack targets the authoritative servers of the victim and floods them with DNS resolution requests through recursive DNS resolvers. This attack is hard to detect, because the resolution requests originates from the legitimate recursive DNS resolvers rather than from the attackers directly.

In more recent news, researchers from Tel Aviv University and the Interdisciplinary Center of Herzliya in Israel found that a new variant of NXNSAttack could cripple servers on a global scale using a botnet comprised of very few computers.[12] Researchers say that NXNSAttack can increase the bandwidth of the infected devices by 1600 times as compared to Mirai, meaning attackers can cause serious damage using far fewer devices.[13]

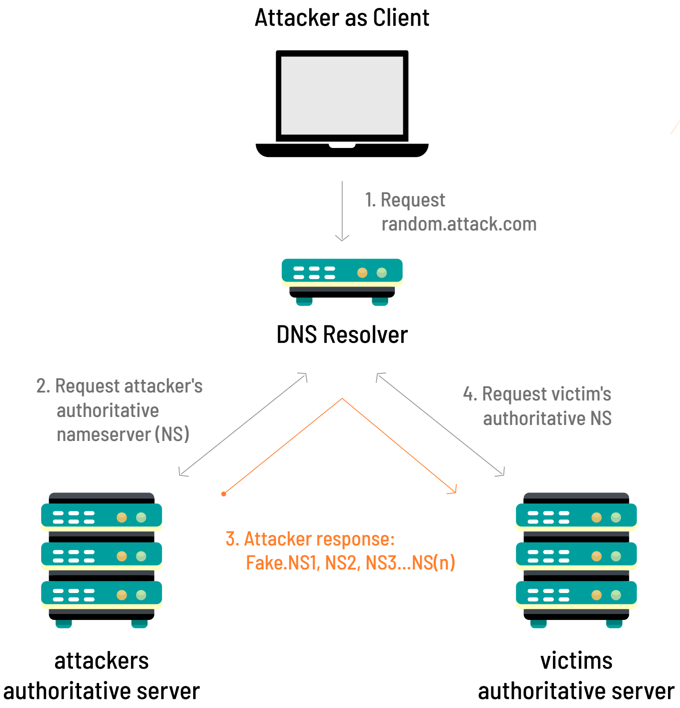
Here's how the NXNSAttack works to take down a victim's server:

1. The attacker sends a request to resolve the domain, say hacker.com, to a recursive DNS server.

2. The recursive DNS server doesn't have the authority to resolve this domain; so it passes the request on to the attacker's malicious authoritative server.

3. The malicious authoritative server then provides a message to the recursive DNS server that states that it has delegated the name resolution operation of a large list of subdomains to the victim's authoritative server.

4. The legitimate recursive DNS server then forwards this DNS query to all the subdomains on the list, creating a huge resolution operation for the target's authoritative server


Attacker as Client
1. Request
random.attack.com
DNS Resolver
2. Request attacker's authoritative nameserver (NS)
4. Request victim's authoritative NS
3. Attacker response: Fake.NS1, NS2, NS3...NS(n)
attackers authoritative server
victims authoritative server

Representation of how NXNSAttack works

Trend 2: The burst attack

Another kind of DDoS attack to be wary of is a burst attack. This attack lasts for a short duration of 30 to 60 seconds wherein the victim encounters a sudden surge in traffic volumes. These short duration burst attacks can span over hours or days with the victim experiencing a ramp-up in traffic, that peaks and then slowly declines all within a minute.

Tackling Burst Attacks

To defend against a burst attack, security administrators should analyze traffic captures, identify the attack signatures, and leverage behavioral-based detection solutions. A security administrator can then manually create rules that block the attack traffic. However, expert attackers don't resort to just one attack vector. Each burst attack can have a different attack vector, making it challenging for IT security personnel to manually set up signatures.

This is where behavior based detection techniques can come to the rescue. This can track and analyze all anomalous requests to connect, and unexpected accesses to files and other resources on the network. This will allow security administrators it to identify potential threats before they begin to spread through the network.

Trend 3: Advanced persistent DoS (APDoS)

APDoS is a major DDoS attack that organizations have to be wary of. APDoS employs around five to eight attack vectors to first launch a massive attack on the network layer. It then bombards the application layers with fraudulent HTTP requests, SQL injection attacks, and XSS attacks at intervals. These attacks can hit an organization with a magnitude of tens of millions of requests per second.

An APDoS attack, as the name suggests, is a persistent attack that can affect a network for weeks at a time and can pose a real challenge for even the most sophisticated security infrastructure. However, there are some ways to fend off an advanced persistent attack. By employing user and entity behavior analytics (UEBA), an organization can identify deviations from normal user behavior. Other best practices like patching software vulnerabilities and updating firewall and antivirus solutions can help fight these threats.

Trend 4: 5G-boosted DDoS attacks

5G has begun slowly making its way into the telecommunications sector and is signaling a huge leap in the speed of access and downloads, offering more bandwidth. While these are certainly major benefits, you can't ignore the elephant in the room: the cybersecurity threats 5G will bring.

Take 5G's offer of greater bandwidth for example; this means that an organization could operate a higher number of IoT devices on the network. This would automatically translate into hackers being spoiled for choice when choosing the initial foothold through which they penetrate the network.

While high volume DDoS attacks don't take place that often, they will certainly have the potential to increase after 5G technology becomes mainstream. What's even more worrying is that with 5G, an attacker only requires a few IoT devices to create a botnet that is capable of paralyzing an organization's servers.[14]

Trend 5: DDoS attacks on cloud environments

The past few years have seen a mass movement of applications and services to the cloud. A cloud environment provides a scalable solution and a user-friendly way for customers to get services and access applications.

Cloud environments can automatically scale up to accommodate an increase in resource usage or an increase in traffic. This could also happen when a malicious attacker is sending phony requests to the cloud service. The cloud service automatically ramps up its computational power and records a higher usage of cloud resources.[15]

This translates into exorbitant bills for cloud users, since cloud service providers charge users based on resource usage. Also, the surge in computational power can be detrimental to the servers operating on the network. A good cloud security solution should be able to employ behavioral-based detection to analyze a potential threat and stop it from infecting the entire cloud network.

Trend 6: DDoS attacks on UDP Memcached servers

Memcache is open-source software that helps website and applications load content faster by storing the content temporarily on devices. This allows the user of the application or website to access content quickly when they return to the site.

Memcache servers have adopted UDP protocol for communication. However, UDP allows data to be sent before the receiver agrees to the communication, which is a vulnerability attackers can exploit. This allows hackers to send spoof requests to the servers, flood them with high volumes, culminating in a server crash.

Memcached attacks in progress can be stopped using the shutdown \ r \ n”, o “flush_all \ r \ n commands so that compromised Memcache servers are disabled.[16] Conducting a thorough review of firewall configurations to check if invalid IPs are blocked are some other ways Memcache DDoS attacks can be mitigated. Apart from this, a comprehensive SIEM solution like ManageEngine Log360 can also help you defend against DDoS.

Defending against DDoS attacks with Log360

Log360 is a one-stop solution for all your log management and network security challenges. This tightly-integrated solution combines the capabilities of ADAudit Plus, EventLog Analyzer, O365 Manager Plus, Exchange Reporter Plus, and Cloud Security Plus. With a versatile combination like this, you'll gain complete control over your network; you'll be able to audit Active Directory changes, network device logs, Microsoft Exchange Servers, Microsoft Exchange Online, Azure Active Directory, and your public cloud infrastructure all from a single console.

Chapter 4: Ransomware - Kidnapping your data

Ransomware is every security admin's worst nightmare and for good reason. Alarmingly the cost of a ransomware attack has increased from $141,000 in 2019 to $283,800 in 2020.[17] Be it a small business or a huge multinational conglomerate, ransomware does not discriminate — it can cause huge losses to a company by encrypting or permanently deleting valuable data.

Ransomware is a constantly evolving threat, and security professionals need to try and always stay one step ahead. In this chapter, we'll discuss the ins and outs of ransomware and the ways to detect and defend against it.

Ransomware is a malware type that encrypts sensitive files or locks up computers, demanding a ransom for the decryption key that makes them accessible again. In 2019, ransomware attacks racked up to 184 million cases worldwide.[18]

Ransomware locks and encrypts important files

A brief history of ransomware

The history of ransomware began in the pre-internet days. In 1989, Joseph Popp, an evolutionary biologist and AIDS researcher, orchestrated the world's first known ransomware attack. He inserted malware, known as AIDS, into floppy disks and sent it to a mailing list of scientists around the world. The malware hid for 90 bootups, and when that threshold was reached, it began to encrypt files on their systems. The victims were welcomed with a message asking them to send $189 addressed to his organization for the files to be released.

However, that did not launch ransomware into the fray of dangerous cyberattacks. It was the internet that truly kick started the ransomware rampage. Since then, ransomware has come in many shapes and sizes and has continually thrown new challenges at cyber security experts.

1. **The true genesis of ransomware**

   When ransomware re-emerged in the mid-2000s, it came armed with stronger encryption technology than its 1989 predecessor. It used RSA encryption, highly secure asymmetric encryption technology used in VPNs, browsers, and email.

   Two types of ransomware attacks were observed — crypto ransomware and locker ransomware. Crypto ransomware encrypts the files and folders on a system and demands a ransom to decrypt it. Locker ransomware locks the user out of their system and then demands a ransom. The ransomware popular during this time were Gpcode, Archiveus, and Krotten.

2. **Money coming in**

   Fast forward 10 years: 2014-15 saw a big jump in the number of ransomware attacks and the amount of money extracted using it. In the mid-2000s, the average ransom for a single attack was $300, and this rose to $500 by 2014. A particularly successful ransomware variant during this time was CryptoLocker, which infected over 250,000 systems and raked in $3 million before it was shut down in a dedicated international effort.

3. **The big heist**

   In 2017, ransomware technology reached new heights with the WannaCry attack. This ransomware could spread through a network without any user interaction. It exploited the vulnerabilities in legacy systems to move laterally through a network. This attack was also notable because it targeted many reputed institutions and businesses such as the NHS in the UK and automobile giants such as Nissan and Renault. In most cases, WannaCry did not even decrypt the files once the ransom was paid.

4. **Gained superpowers**

   Ryuk is ransomware that emerged in 2018, but it evolved into a dangerous threat only a year later. Ryuk has one of the most advanced propagation techniques seen in ransomware history. It uses certain bots to steal user credentials even before the Ryuk malware itself is downloaded on to the system. It conducts targeted attacks on large companies and government institutions. Between 2018-19, hackers leveraged Ryuk to steal around $5 million.

5. **Diversifying operations**

One of the latest entries into the ransomware arena is SNAKE ransomware, which has already targeted big names such as the auto manufacturer Honda and the European power company Enel. SNAKE, also known as Ekans, follows the usual formula of encrypting files and then demanding a ransom. However, its targets are not regular Windows or Linux systems, but Industrial Control Systems (ICS).

If this ransomware variant is allowed to spread through these systems, it can completely halt the operations of organizations and hefty sums of ransom would be demanded. SNAKE uses a non-secure remote desktop protocol (RDP) connection to infiltrate a network. With most employees working from home and utilizing non-secure connections, the threat of this ransomware is more serious than ever.

Ransomware and your business

Businesses should be worried about ransomware, because the numbers don't paint a pretty picture. If the sheer number of ransomware attacks doesn't not make you sit up straight, these numbers definitely will:

1. Global costs of ransomware attacks are projected to touch $20 billion in 2021.[19]

2. If you are in the healthcare sector, you are number one on the ransomware hit list. Ransomware attacks have cost US healthcare organizations $157 million since 2016.[20]

3.The average downtime for a company after a ransomware attack is 9.6 days.[21] Downtime costs are generally five to ten times more than the ransom amount.[22]

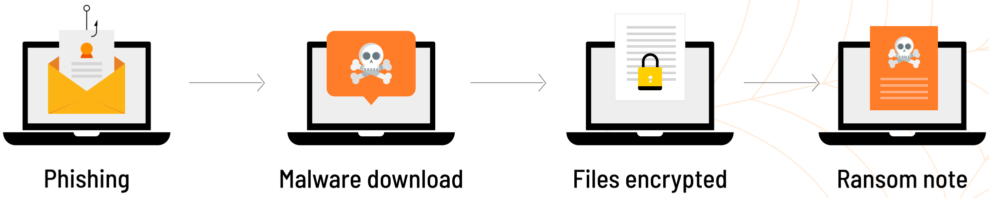
Ransomware can spell huge losses for an organization under normal circumstances. But in the current pandemic situation, a ransomware attack can be the final nail in the coffin for many businesses.

Ransomware on the rise during the COVID-19 pandemic

The pandemic has naturally provided fertile ground for all cyberattacks, including ransomware. Combine the anxiety levels with the barely protected devices used by remote employees to connect to corporate networks, and it's the perfect recipe for an attack.

Ransomware attacks have been especially targeted against healthcare institutions, which are particularly vulnerable right now. Attackers have also reportedly used information related to COVID-19 to lure people to click on malicious links. Apart from the business loss, these attacks can hamper the response to the pandemic, causing further harm to an already anxiety-ridden world.

Breaking down a ransomware attack

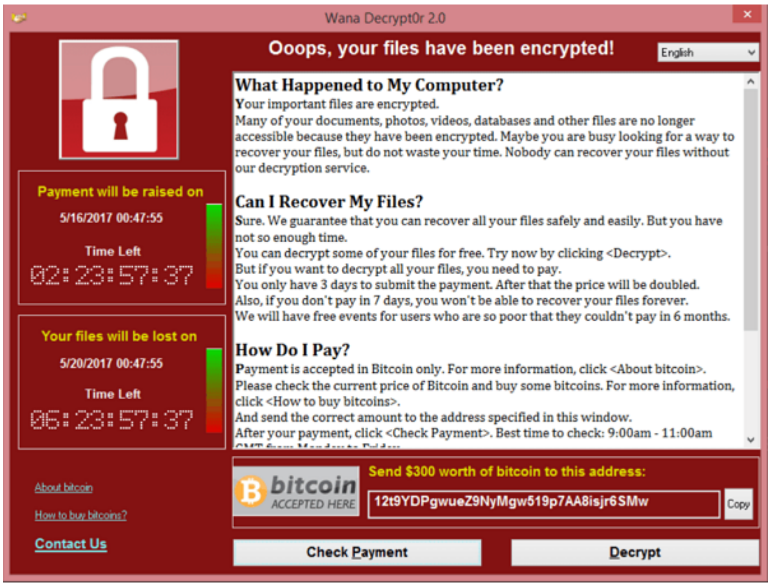


There are four main stages of a ransomware attack: i) Initial access through phishing, ii) Downloading of malware, iii) Encryption of files, and iv) A ransom note.

Generally, ransomware enters a system by way of phishing emails, malicious websites, or random pop-ups, which try to bait the average internet user. However, more recent ransomware variants prefer tailor made attacks that almost always dupe the targeted victim. For example, an employee of a company might receive a phishing email that is purportedly from their boss. The employee clicks a link in the email and snap! Malware begins to download and the computer is infected.

Malware has to act fast before it is detected by the system's security controls. So, it immediately starts encrypting data within the system it has initially infected. Ransomware can also rename files, modify them, and sometimes even permanently delete them. Ransomware such as WannaCry and NotPetya also spread laterally through a network by exploiting system vulnerabilities that have not been patched.

When the victim starts up the system, they will not be able to open any important folders. A message might pop up asking them to pay a certain amount of money in cryptocurrency such as Ethereum and Zcash, which are harder to trace. And the victim may or may not get their files back because, in 25% of the ransomware cases, the files are never decrypted.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Screenshot of the WannaCry ransom note

While these are the general lines along which a ransomware attack happens, recent attacks have been much more sophisticated. They are expected to get even more sophisticated in the future.

Future trends in ransomware

Since ransomware will always be an IT administrator's worst nightmare, it helps to know what shape the threat will take in the coming years. Here are three ransomware trends we will see in the future.

1. **IoT devices will be targeted**
   Gartner projects that there will be 25 billion connected devices by the end of 2021.[23] Stats also indicate that workplaces are increasingly going the IoT way. However, IoT devices aren't the most secure devices, because they do not have to adhere to any universal security standard yet. People generally underestimate this threat, because a thermostat cannot leak sensitive data. But it's never as simple as that.

   While IoT devices do not contain data the way a computer does, attacks on IoT devices pose a more dangerous threat. If an attacker hacks into and gains control of the device, the danger moves from an online space into the physical world. For example, if ransomware has gained control over your home's security system, the attacker could threaten to unlock your house while you're away on holiday, leaving your house open to actual burglars. What if someone aimed an attack at a pacemaker? It would land the victim in a literal life or death situation.

   As IoT leads our lives into an entirely new future, it also naturally presents us with unprecedented problems, which need to be dealt with in newer, more creative ways.

2. **Increased use of ransomware as a service (RaaS)**
   Ransomware as a service is the evil alter ego to software as a service (SaaS) applications. RaaS enables even a novice hacker to launch ransomware attacks on their own. On the dark web, ransomware codes are available for as little as $10. This would exponentially increase the number of ransomware attacks.

3. **Ransomware will not stop with just encryption**
   Ransomware attackers now have new threats up their sleeves. They attack a few big businesses or government institutions and threaten to publish their sensitive information online unless they pay huge ransom amounts. Since most big businesses would rather pay the money and recover their data, the attackers almost always get their prize.

Some ransomware also install multiple payloads on a system -- while one payload could performs the encryption, the other payloads get busy stealing valuable data such as credentials, and send them to the attacker. The attacker could then sells them on the dark web. So even if the ransom is paid, the user's credentials are out on the internet.

The solution for the ransomware challenge

Often, tracing ransomware attackers is a wild goose chase as they are smart at covering their tracks.However, organizations should take security more seriously and use tools that can amp up their game. Here are four deceptively simple, but often ignored steps that you can implement right away:

1. **Backups, backups, backups**
   You can never perform too many backups. Backing up important data in external storage can help organizations sail through a ransomware attack with minimal damage to their operations.

2. **Old isn't gold**
   Many recent ransomware variants spread through networks via systems that were unpatched for known vulnerabilities. Regularly update and patch all your systems, and don't leave any legacy software lying around. If you can't afford to lose your legacy systems, make sure that they are monitored rigorously for any abnormal activity.

3. **No careless clicking**
   Conduct awareness programs for your employees, and make it easy for them to follow security best practices. Aren't we all tired of hearing that humans are the biggest threat to data security?

4. **Invest in threat detection tools**
   Nothing can beat the efficiency of a threat detection tool that constantly keeps tabs on all your network activity and alerts you of any suspicious events on your network. Combined with the best practices listed above, this will ensure that your organization is well-prepared to handle any ransomware attack.

Chapter 5: Cryptojacking - Cryptomining's evil alter-ego

When was the last time you checked the processes running on your network? Probably so long ago that you don't remember. Usually, we leverage Ctrl + Alt + Del when we need to quit a frozen program. But what if there are malicious processes running on your computer that you're completely unaware of?

Sometimes, these malicious processes could even take on the names of legitimate Windows processes. If these programs secretly mine cryptocurrency through your computer, then you have unfortunately met with a cryptojacker. The sooner you detect and mitigate these processes, the longer your computer will live.

Cryptojacking is basically illegal cryptomining. Cryptomining is the legitimate process by which cryptocurrency is mined on the internet. Mining cryptocurrency entails using the processing power of computing devices to solve complex mathematical programs, at the end of which, the miner is rewarded with a block of cryptocurrency.

However, as more and more people began mining, the process became more competitive and exclusive. Many miners saw cryptomining becoming less profitable as the cost of mining increased manifold over the years. Some of them turned to cryptojacking to keep those coins coming, but at someone else's expense.

The first half of 2019 saw 52.7 million cryptomining attacks.[24] In 2020, cryptojacking morphed into a bigger threat because of the sheer number of attacks and a big evolution in attack tactics. Let's take a quick look at the brief history of cryptojacking to see how far it has come and make intelligent predictions about what lies ahead in this very 21st century problem.

History of cryptojacking

Cryptojacking attacks made the news in mid-2017, when cryptocurrency entered mainstream use and gained legitimacy. However, there were also several other reasons for the popularity of cryptojacking, the launch of Coinhive being one of them. Coinhive was a cryptocurrency mining service that published a script for mining a cryptocurrency called Monero.

Bitcoin mining currently requires very powerful machines called Application Specific Internet Circuits (ASCI). Other coins like Monero do not require such a huge initial investment in hardware. However, any kind of mining drastically shortens the lifespan of a machine and incurs high electricity bills. To avoid these consequences, miners use other peoples' machines to do the job.

Here are some of the most notable cryptojacking attacks:

1. **Wannamine:**
   This attack from 2017 was one of the first widely reported cryptojacking attacks. Once Wannamine infects a computer, it runs code that execute complex mathematical problems to mine Monero. Like WannaCry, the ransomware attack, Wannamine uses certain vulnerabilities in Windows systems to spread malware across entire networks of computers.

2. **Ghostminer:**
   The same year saw a new way of dropping cryptomining malware into systems: Fileless malware. Fileless malware does not download as a file into a system and rather piggybacks on a legitimate program that antivirus software do not suspect. Ghostminer exploited the legitimate Windows program, Windows Management Instrumentation (WMI), to avoid detection.

3. **PSMiner and Cookieminer:**
   In 2019, two new strains of cryptomining malware were discovered: PSMiner for Windows and Cookieminer for Mac. PSMiner used the now familiar trick of hiding behind PowerShell scripts on Windows. But Cookieminer was new — it did not stop with just installing cryptomining software on the devices, but it went one step further and stole browser cookies from devices as well. The stolen cookies were associated with major cryptocurrency exchanges. The hackers could then use these cookies to impersonate the victim and conduct transactions in the victim's name.

Most cryptomining malware, when detected by organizations, simply slink back into the dark web. They then upgrade their techniques and come back into attack mode.

Impact of cryptojacking on businesses

The global cryptomining market is growing at an annual compound rate of 29.7%.[25]
All businesses are prime targets for cryptojackers because they possess multiple systems with enterprise-level computing capabilities, which is just what they need.

If an network is cryptojacked, it will first affect business operations before affecting the employees. Unlike ransomware, cryptojacking malware can go undetected for months or years, causing terribly high electricity bills and, even worse, completely wearing out expensive systems, which will need to be replaced.

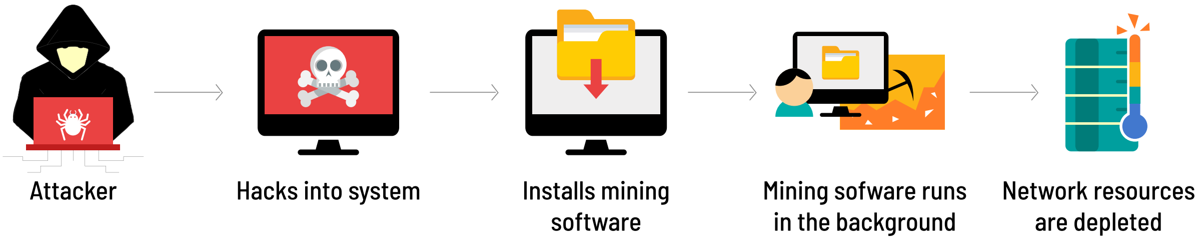
Cryptojacking also makes a network vulnerable to other cyber attacks, as it lays open critical access points that can be used by other hackers.

How Cryptojacking works

There are two variants of cryptojacking: i) Downloaded malware, and ii) Browser-based mining.

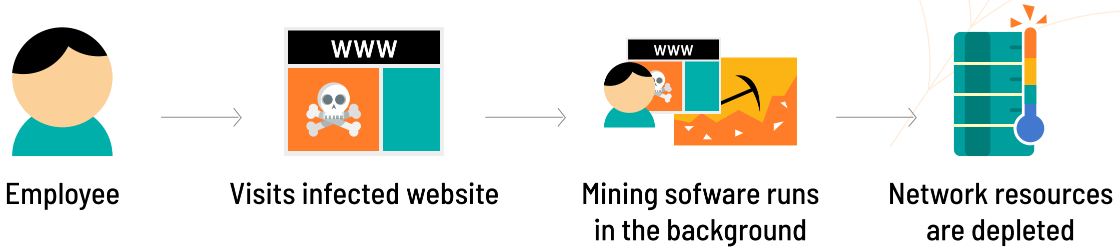
- **Downloaded malware**
  The attacker employs social engineering tactics to send genuine-looking phishing emails, which contain malicious links or that lure people into malicious websites. Once the victim clicks on the link, a code is run, which delivers the malware delivery on to their system. The cryptomining software then surreptitiously works to mine cryptocurrency in the background while you go about your work.

  Cryptojacking scripts are designed to work without interrupting the user's activities. Cryptojacking infects computer networks because they can be used to make a cryptomining pool whereby each of the computers contribute only a small amount of processing power. This can keep the attack from being detected for months or even years.


Attacker
Hacks into system
Installs mining software
Mining sofware runs in the background
Network resources are depleted

Cryptojacking after the download of a malware

- **Browser-based mining**
  In this variant, the attacker plants cryptomining code on to the javascript of a website. This code runs every time a user visits the website and it uses the computing powers of the system to mine cryptocurrency for the website. While this can be a legitimate way for websites to make money out of the traffic on their website, most of the time, the website owners are unaware of the code insertion.


WWW
WWW
Employee
Visits infected website
Mining sofware runs in the background
Network resources are depleted

Cryptojacking after browser-based mining

Future trends of cryptojacking

Here are some trends of cryptojacking that we can expect to see in the years to come.

- **More targeted phishing**
  Cryptojackers are becoming smarter with their phishing techniques. This means that they will use social engineering to attack in a more targeted fashion and this will lead to more people being fooled and more money for hackers.

- **Cryptojacking leading to a data breach**
  So far, cryptojacking has rarely been connected with a data breach. Future cryptomining malware might also have other tricks up its sleeve, such as stealing credentials after dropping malware-laden payloads into a system. Once credentials are stolen, a data breach can occur at any time.

- **Increasing value of certain cryptocurrencies**
  Many experts rejoiced the fall of Coinhive, as they believed it would take the life out of Monero mining. However, many websites still carry Monero-mining scripts. Some experts also say that any drop in the value of Monero will increase interest in other cryptocurrencies that can be mined on regular CPUs. This is particularly relevant because cryptojackers are interested in the same currencies.

Defending against cryptojacking

Following security best practices will keep you safe from a lot of the cyberattacks that are floating around on the internet. Making your employees aware of the risks and convincing them to follow best practices while online will help prevent careless clicking on malicious links or ads.

Here are some proactive measures that can be taken specifically to defend against cryptojacking:

- **Use a cryptomining blocker:**
  There are various cryptomining blockers available as extensions to internet browsers. These can be very helpful against browser-based cryptojacking attempts.

- **Monitor the CPU and GPU usage:**
  Very high CPU usage is one of the major signs that a system has been cryptojacked. CPU usage can be continuously monitored by network security tools and SIEM solutions.

- **Monitor your websites:**
  Constantly monitor your websites for any cryptomining malware embedded in them. In most cases of browser-based mining, the website owners were completely unaware of the malware on their website. Also, in many cases, the malware was present in third-party plug-ins on the website, which are harder to monitor but should never be overlooked.

one-size-fits-all approach doesn't work. You need to list your business requirements, the risks your business faces, and the level of security you're trying to achieve, and then choose the best SIEM solution that fits your requirements.

Log360, a comprehensive SIEM solution that has a flexible architecture and customizable components, is a great choice for businesses of all sizes.

Read on to learn about how Log360 helps mitigate the threats and attacks described in this e-book.

Before we go ahead, we suggest you do a risk assessment of your organization. A comprehensive risk assessment will let you know your business's risk appetite. This will also help you allocate an appropriate budget to invest in a solution that can mitigate major risks.

Conducting a risk assessment
If you're looking for a quick and easy way to conduct a risk assessment of your business, check out this post on **How to conduct an effective risk assessment for your healthcare organization.**"

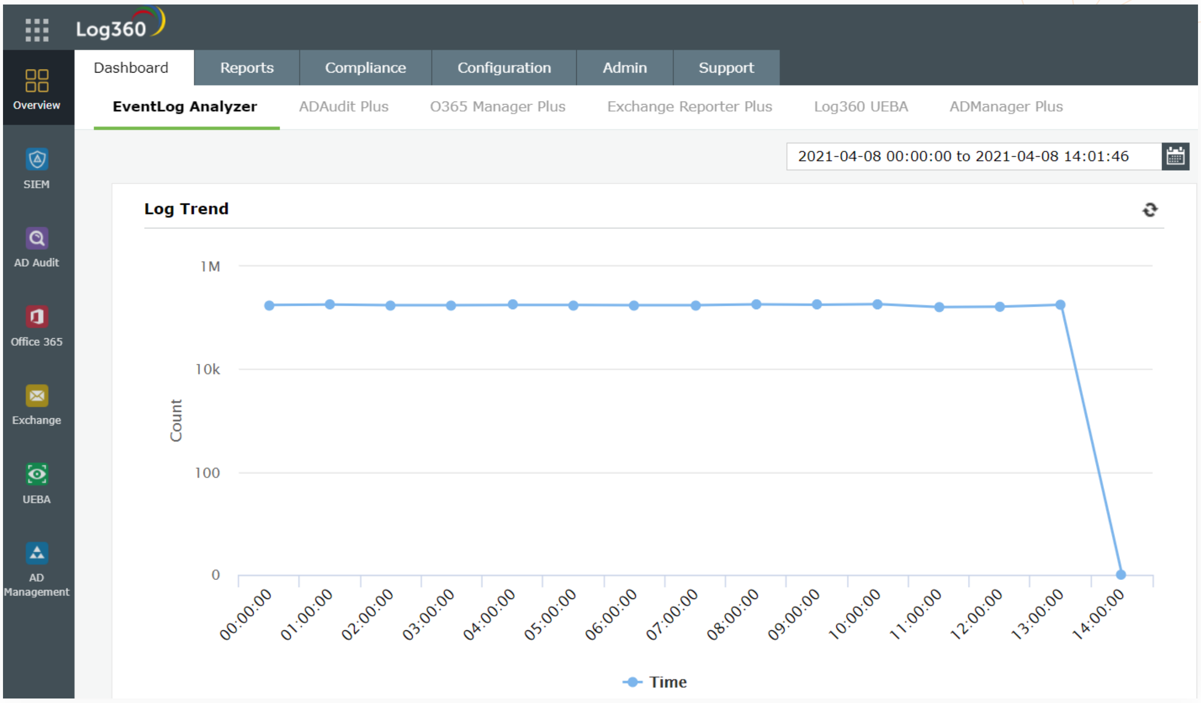
While this article is tailored for a healthcare environment, the steps can be applied to any business environment.

Manageengine Log360 is a comprehensive solution that enables businesses to detect and mitigate threats to their IT environment.

Since you're familiar with the threats we've discussed above, this next section will focus on how Log360 can help mitigate these threats.

Log360 against DDoS, cryptojacking, and ransomware

Log360 brings to you a central console that gives you a 360-degree view of security events happening in your network. With Log360, you can correlate threat indicators that have occurred across the network to stop DDoS, cryptojacking and ransomware before they cause damage.



Log360 dashboard showing the activity count over time and general health of a network

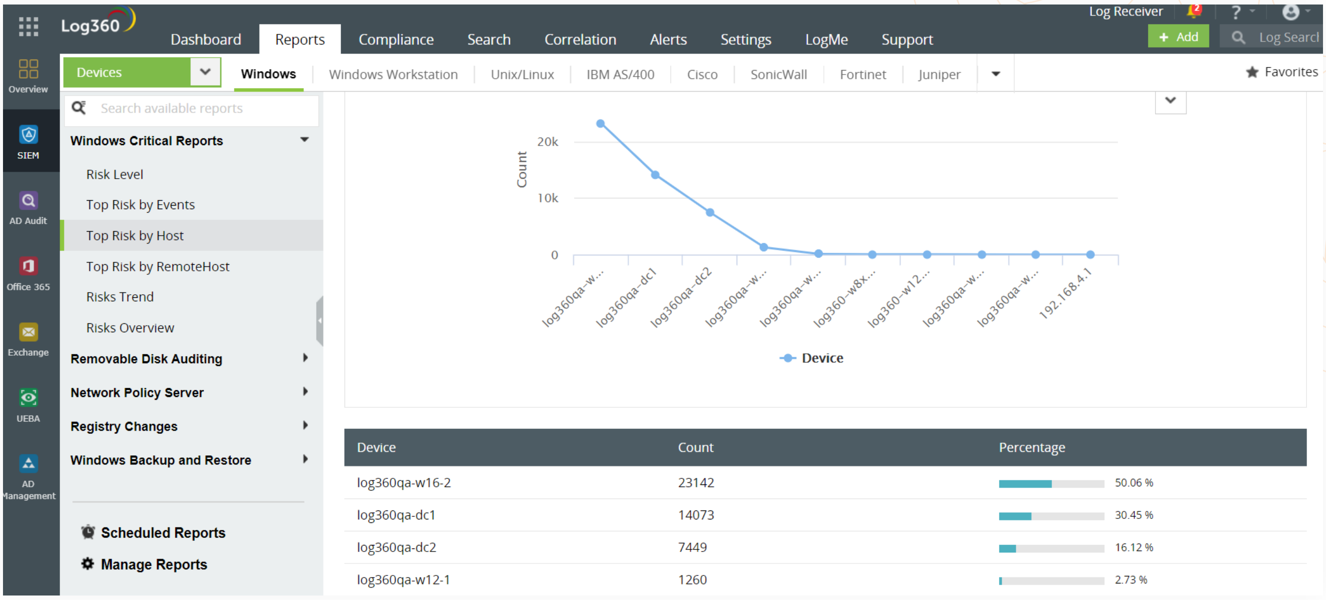
Log360 is handy at detecting suspicious activity on your webserver, databases, applications and network devices. An attacker could be trying to take control of confidential information on your systems, install shady cryptomining software, or raise a legion of infected systems to exhaust your server.

Log360 helps you deal with any malicious activity by providing crucial and intuitive insights. These insights are presented in the form of easy-to-understand reports.

The solution classifies reports into three categories:

1. **Top reports:**

   Reports that give you an inside look into the top user activities that likely pose a risk. like what sort of websites are being accessed by users and how they're accessing them. You can also view what kind of activity or events on your network pose a risk.

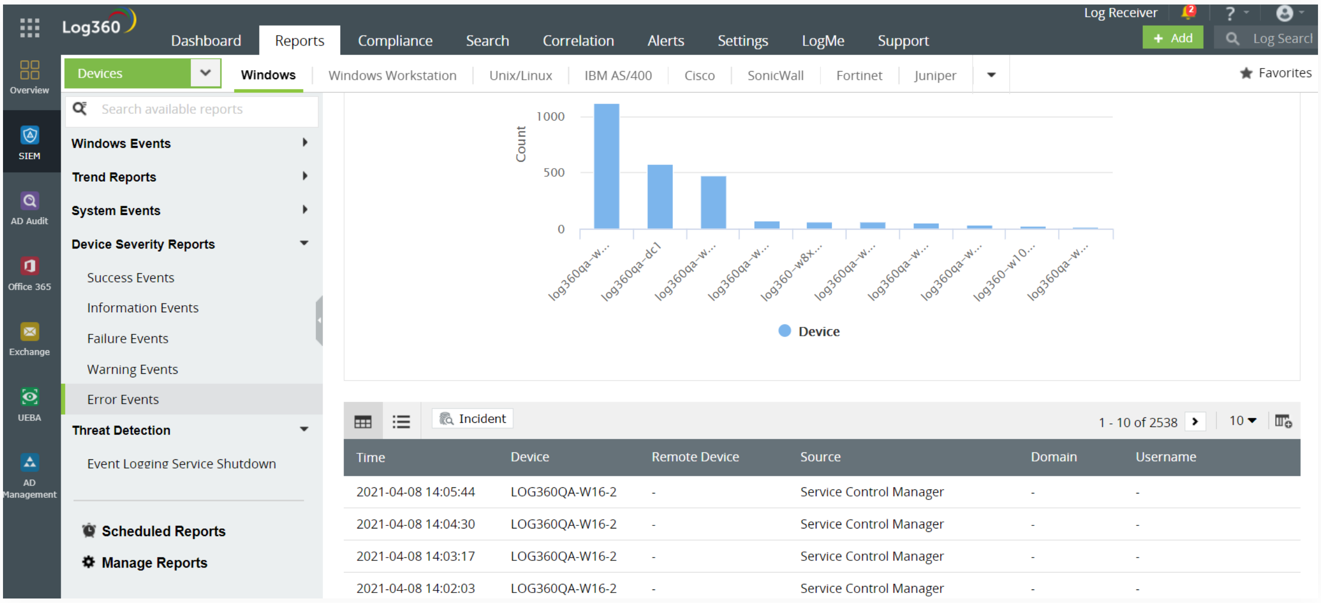


Device	Count	Percentage
log360qa-w16-2	23142	50.06 %
log360qa-dc1	14073	30.45 %
log360qa-dc2	7449	16.12 %
log360qa-w12-1	1260	2.73 %

The Top Risk by Host report in Log360

2. Error reports:

These reports display errors a user has encountered on the network. These could be errors encountered while running an application or a system event error.

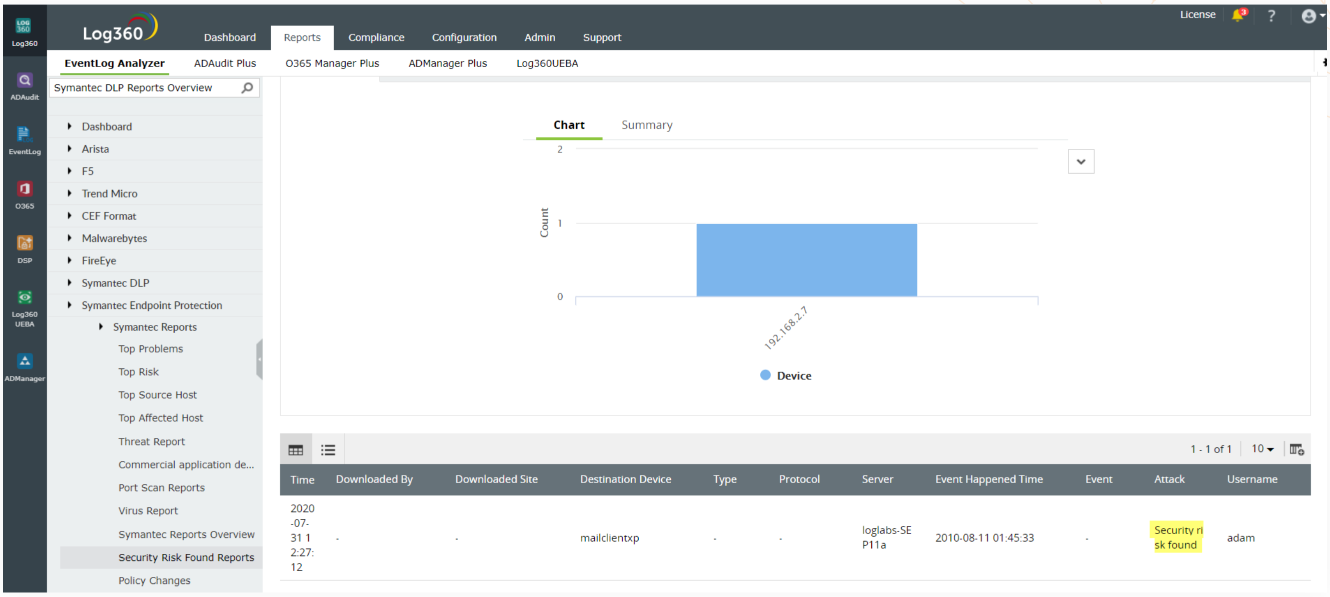


Time	Device	Remote Device	Source	Domain	Username
2021-04-08 14:05:44	LOG360QA-W16-2	-	Service Control Manager	-	-
2021-04-08 14:04:30	LOG360QA-W16-2	-	Service Control Manager	-	-
2021-04-08 14:03:17	LOG360QA-W16-2	-	Service Control Manager	-	-
2021-04-08 14:02:03	LOG360QA-W16-2	-	Service Control Manager	-	-

A sample report on Error Events based on Source in Log360

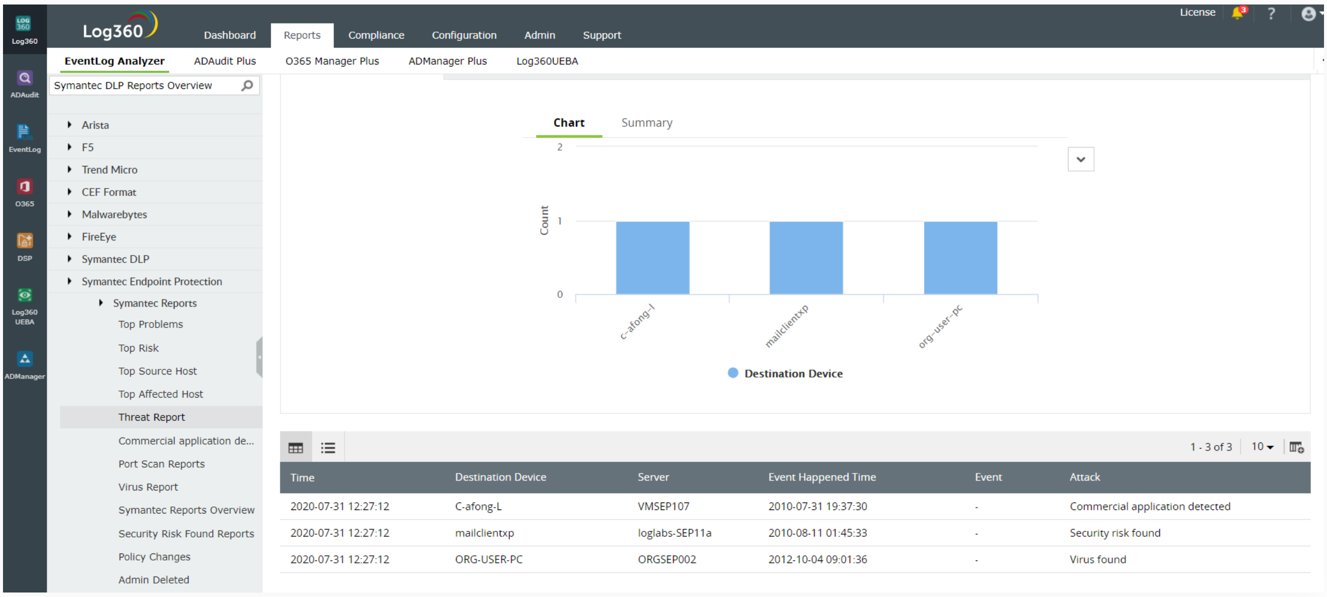
3. Attack reports:

hese reports show attempted attacks on your network. You have out-of-the-box reports on different types of attacks that may have taken place on your network, including threats that were stopped by firewalls and antivirus software.



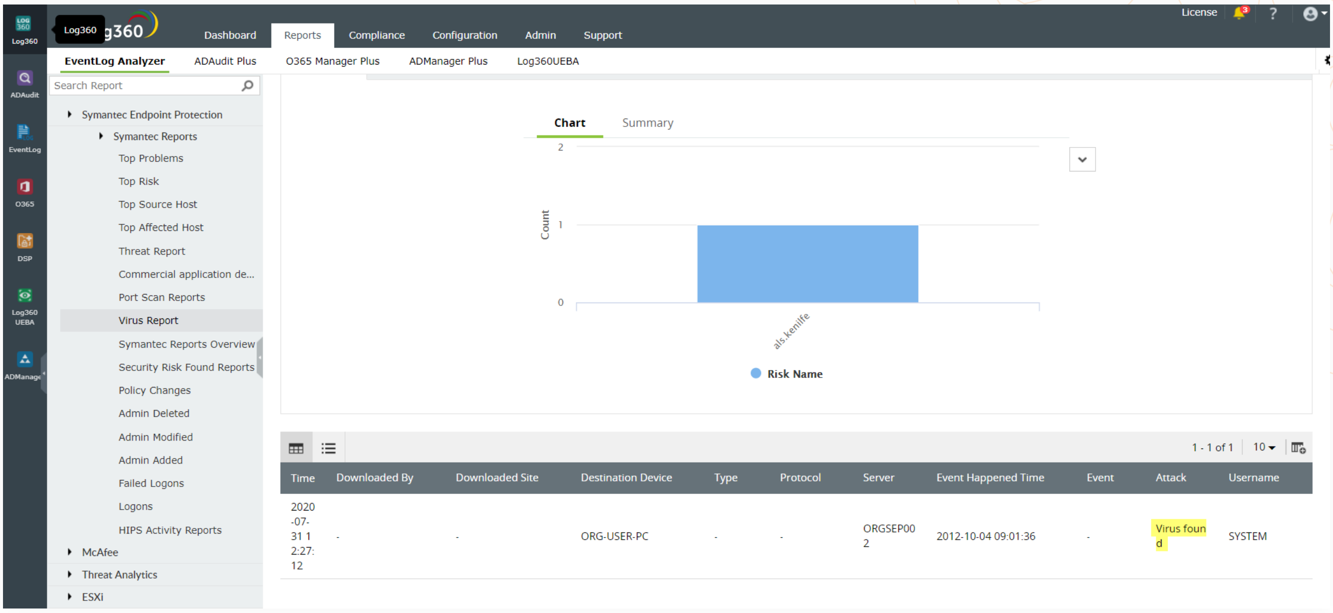
Time	Downloaded By	Downloaded Site	Destination Device	Type	Protocol	Server	Event Happened Time	Event	Attack	Username
2020-07-31 12:27:12	-	-	mailclientxp	-	-	loglabs-SEP11a	2010-08-11 01:45:33	-	Security risk found	adam

Security Risk Found report in Log360



Time	Destination Device	Server	Event Happened Time	Event	Attack
2020-07-31 12:27:12	C-afong-L	VMSEP107	2010-07-31 19:37:30	-	Commercial application detected
2020-07-31 12:27:12	mailclientxp	loglabs-SEP11a	2010-08-11 01:45:33	-	Security risk found
2020-07-31 12:27:12	ORG-USER-PC	ORGSEP002	2012-10-04 09:01:36	-	Virus found

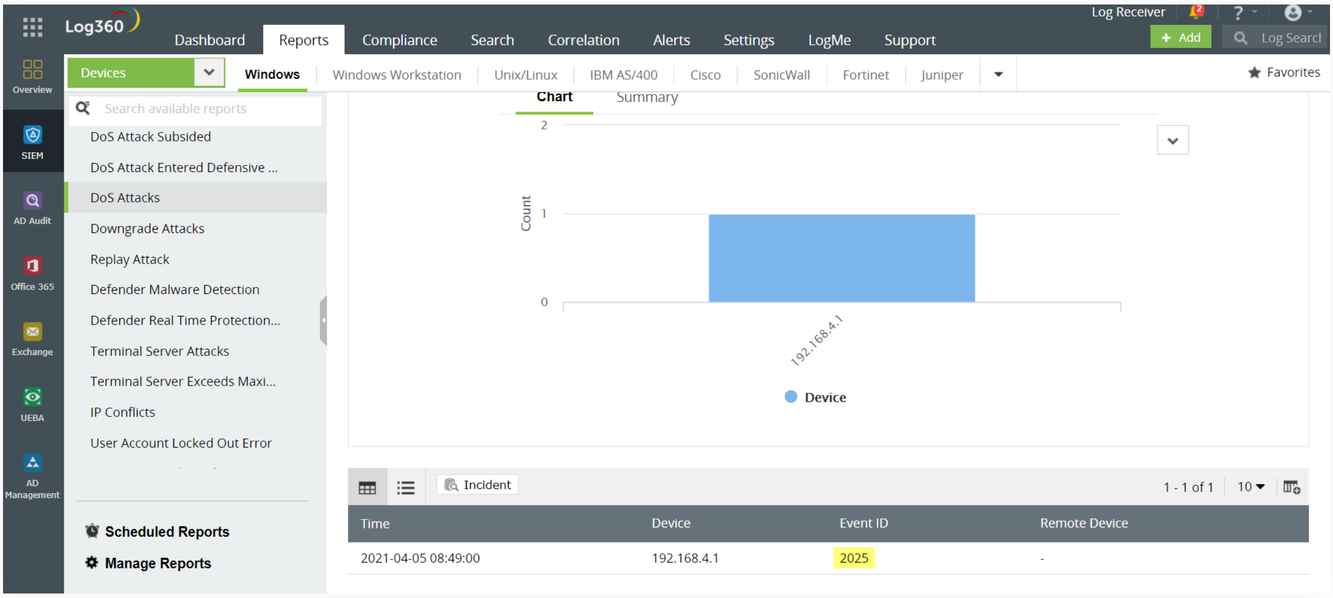
Threat Report identified by Symantec Endpoint Protection available in Log360



Time	Downloaded By	Downloaded Site	Destination Device	Type	Protocol	Server	Event Happened Time	Event	Attack	Username
2020-07-31 12:27:12	-	-	ORG-USER-PC	-	-	ORGSEP002	2012-10-04 09:01:36	-	Virus found	SYSTEM

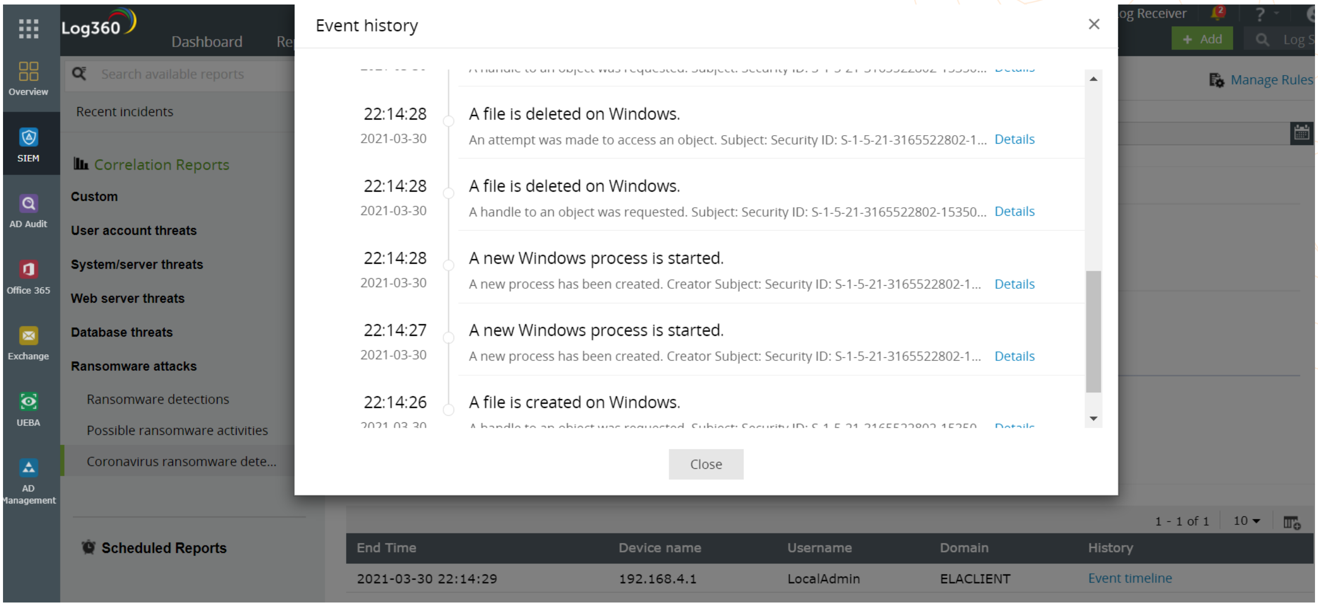
Log360's Virus Report shows viruses found in the network

Log360 also provides specific reports about possible DDoS, ransomware and cryptojacking attacks on the network.



Time	Device	Event ID	Remote Device
2021-04-05 08:49:00	192.168.4.1	2025	-

Log360 detecting a possible DoS attack on the network

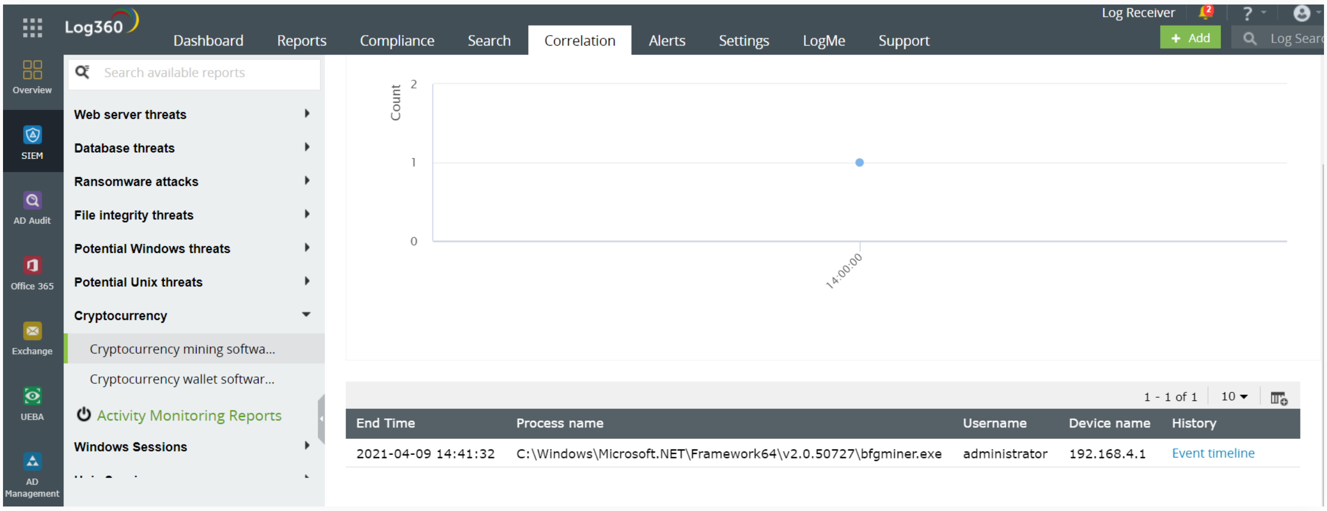


Event history

	A handle to an object was requested. Subject: Security ID: S-1-5-21-3165522802-15350... Details
22:14:28 2021-03-30	A file is deleted on Windows. An attempt was made to access an object. Subject: Security ID: S-1-5-21-3165522802-1... Details
22:14:28 2021-03-30	A file is deleted on Windows. A handle to an object was requested. Subject: Security ID: S-1-5-21-3165522802-15350... Details
22:14:28 2021-03-30	A new Windows process is started. A new process has been created. Creator Subject: Security ID: S-1-5-21-3165522802-1... Details
22:14:27 2021-03-30	A new Windows process is started. A new process has been created. Creator Subject: Security ID: S-1-5-21-3165522802-1... Details
22:14:26 2021-03-30	A file is created on Windows. A handle to an object was requested. Subject: Security ID: S-1-5-21-3165522802-15350... Details

End Time	Device name	Username	Domain	History
2021-03-30 22:14:29	192.168.4.1	LocalAdmin	ELACLIENT	Event timeline

Log360 showing a possible infection by the new Coronavirus ransomware and the timelilne of attack



End Time	Process name	Username	Device name	History
2021-04-09 14:41:32	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\bfgminer.exe	administrator	192.168.4.1	Event timeline

Log360 showing instances of possible cryptojacking attempts

Ready to get started with Log360?

Download

If you're still unsure, take your time and explore Log360 using a personalized demo.

Schedule a personalized demo

Endnotes

1. DDoS Attacks Jump 542% from Q4 2019 to Q1 2020, June 2020, https://www.darkreading.com/threat-intelligence/ddos-attacks-jump-542--from-q4-2019-to-q1-2020/d/d-id/1338208.

2. Threat Hunter Team, Symantec, "Threat Landscape Trends – Q2 2020," Symantec, August 2020, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-trends-q2-2020.

3. Casey Cran, "The 2020 ransomware resiliency report," https://go.ninjarmm.com/2020-ransomware-resiliency-report/.

4. Stephane Nappo, "Stepahen Nappo quotes," Goodreads.com, https://www.goodreads.com/author/quotes/19698507.Stephane_Nappo.

5. Jennifer Steve, "Types of DDoS attacks and their prevention and mitigation strategy," EC-Council Blog, December 2019, https://blog.eccouncil.org/types-of-ddos-attacks-and-their-prevention-and-mitigation-strategy/.

6. Oleg Kupreev, Ekaterina Badovskaya and Alexander Gutnikov, " DDoS attacks in Q1 2020," SECURELIST by Kaspersky, https://securelist.com/ddos-attacks-in-q1-2020/96837/.

7. Ibid.

8. Ibid.

9. Ibid.

10. Michael Novinson, "8 DDoS attack trends to watch for in 2020," September 2019, https://www.crn.com/slide-shows/security/8-ddos-attack-trends-to-watch-for-in-2020/9.

11. Catalin Cimpanu, "NXNSAttack technique can be abused for large-scale DDoS attacks," May 2020, ZDNET, https://www.zdnet.com/article/nxnsattack-technique-can-be-abused-for-large-scale-ddos-attacks/.

12. EurekaAlert, "Tel Aviv University and IDC Herzliya researchers thwart large-scale cyberattack threat," May 28, 2020, https://www.eurekalert.org/pub_releases/2020-05/afot-tau052820.php.

13. Yehuda Afek, Anat Bremler-Barr and Lior Shafir, "NXNSAttack: Recursive DNS inefficiencies and vulnerabilities," USENIX, https://www.usenix.org/system/files/sec20-afek.pdf.

14. Sean Newman, "5g will increase DDoS attack risk," Corero, https://www.corero.com/blog/5g-will-increase-ddos-attack-risk/.

15. Joshua Osborn, "DDOS attacks-Seven effects it has on cloud environments," Comparethecloud.net, https://www.comparethecloud.net/articles/ddos-attacks-seven-effects-it-has-on-cloud-environments/.

16. Memcached DDoS explained, Akamai, https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/ddos-reflection-attack-memcached-udp.jsp.

17. Eric C, "Ransomware facts, trends & statistics for 2020," April 2020, Safety Detectives, https://www.safetydetectives.com/blog/ransomware-statistics/.

18. Juliana DeGroot, "A history of ransomware attacks: The biggest and worst ransomware attacks of all time," Data Insider, December 1, 2020, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

19. Steve Morgan, "Global ransomware damage costs predicted to reach $20 billion (USD) by 2021," Cybercrime Magazine, October 21, 2019, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.

20. Paul Bschoff, "172 ransomware attacks on US healthcare organizations since 2016 (costing over $157 million)," Comparitech, February 2020, https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/.

21. Jessica Davis, "Ransomware costs on the rise, causes nearly 10 days of downtime." Health ITSecurity, July 16, 2019, https://healthitsecurity.com/news/ransomware-costs-on-the-rise-causes-nearly-10-days-of-downtime.

22. Ransom amounts rise 90% in Q1 as Ryuk increases, Coveware, April 16, 2019, https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases.

23. Gartner identifies top 10 IoT technologies and trends, Gartner, November 7, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

24. Yessi Bello Perez, "Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019," TNW, July 21, 2019, https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/.

25. The new gold rush isn't gold, Cision, June 23, 2020, https://www.prnewswire.com/news-releases/the-new-gold-rush-isnt-gold-301081595.html.

ManageEngine
Log360

ManageEngine Log360, a comprehensive SIEM solution helps enterprises to thwart attacks, monitor security events, and comply with regulatory mandates. The solution comes bundled with a log management component that provides better visibility into network activity, incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents, ML-driven user and entity behavior analytics add-on that baselines normal user behaviors and spots anomalous user activities, threat intelligence platform that brings in dynamic threat feeds for security monitoring and aids enterprises to stay on top of attacks.

For more information about Log360, visit manageengine.com/log-management.

$ Get Quote   ⤓ Download