Threats of the Year

A look back at the tactics and tools of 2019

CISCO

Contents

The Targets and Tools of 2019

Some cybercriminals have specific organizations in mind when they're planning an attack. For whatever reason, they know who they want to breach, and the potential rewards to be gained. Very little deters them from their goal. Take the global targeted ransomware attacks that took place this year; the effects were so destructive, partly because the organizations were deliberately selected from the firing line.

For other cybercriminals, it's more of a numbers game. They are looking to hit as many victims as possible without regard for which organizations or individuals they affect, as long as they get their end result.

For example, the emergence of DNS hijacking this year saw threat actors take charge of certain DNS entries. This allowed attackers to silently redirect unsuspecting visitors from legitimate systems to malicious ones, potentially to install malware or to intercept confidential data and credentials.

In this roundup, we'll take you on a journey through our investigations over the past year, highlighting six noteworthy threats. You can read more in-depth analyses on our Threat of the Month blog and sign up to receive future updates on what 2020 brings us in the threat landscape.

With our recommendations at the end of this report, you can use this retrospective in any security-focused board meetings or business planning sessions you're holding over the next few months to guide you on the tools and processes you need. It can serve as a resource to help explain how your current security posture would cope with an attack, and identify any gaps. Understand how quickly you could respond to each of these six threats? When would you know about the threat? And what do you need to do to improve your time to respond.

From remote access trojans, to hiding threats in encrypted traffic, we've seen various innovations in how the bad guys are seeking to evade detection.

1. DNS Hijacking

DNS, or to give it its full name, the Domain Name System, is the core technology that translates human readable domain names (e.g., www.example.com) into machine-readable IP addresses (an X-digit number punctuated like this-208.67.222.222). Think of using DNS like asking a librarian for help locating a book; you type in a text name and the DNS "librarian" translates this into an IP address, searches the bookshelves for the corresponding IP address, and brings you back the website that you're looking for.

The scenario

You log into your company's network at 9 a.m., and the first thing you do after your morning coffee is check your industry's news. You open your browser, click on the bookmark, and expect to arrive at your favorite news site.

Except that's not the website you end up visiting.

Cisco Talos, Cisco's threat intelligence group, has been watching DNS very closely, and this year we spotted multiple attacks relying on DNS hijacking.

The thing about DNS attacks is that they don't go directly after their intended target (you at your desk). Rather, they attack the librarian (in this case, the industry news website you were hoping to read over coffee). Instead of sending you to the correct location where your book resides, the librarian instead sends you somewhere entirely different. The worst thing is, you may not know it. The fake site, or the book you pull off the shelf, may look like what you wanted, but actually be something entirely different – the supposed children's book turns out to be the Anarchist Cookbook instead.

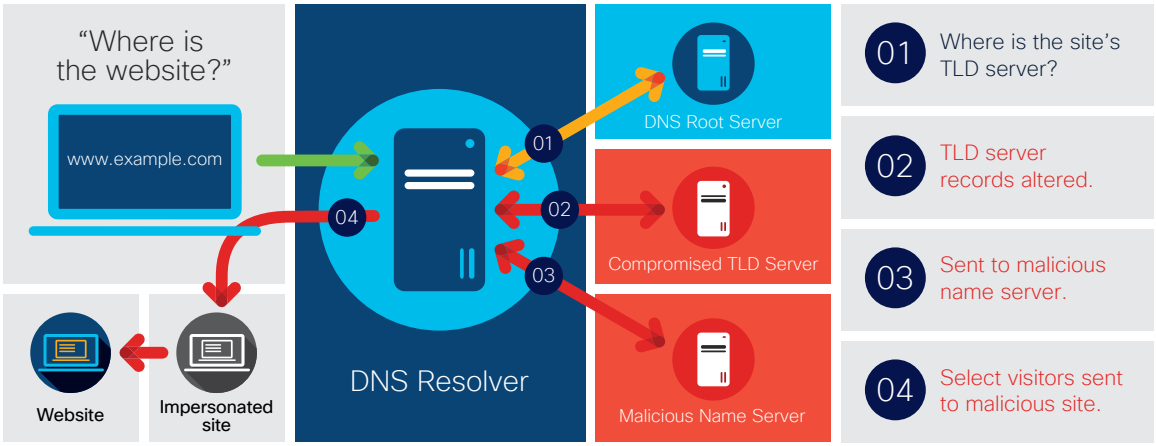
The attack comes down to the cybercriminal altering the directions to a legitimate website to lead to a malicious one. You ask for the IP address of a particular domain you want to visit, but the DNS records were tampered with so that you are sent to a malicious IP address instead. The attacker can then pick and choose what to do with you as a victim when you arrive unsuspecting at the malicious server. The attacker could attempt to install malware, collect your username and password, or invisibly act as a go-between with the legitimate site and intercept all data you access to use for other purposes (i.e., identity theft, ransom, etc.).

Sea Turtle starts to swim

Sea Turtle is an example of DNS hijacking that went after the organizations that control TLD (top-level domains). The attacker exploited multiple vulnerabilities to take control of the name servers for entire domains.

This approach gives the attackers control over the IP addresses returned for DNS requests. Setting up a malicious name server, the attacker can choose when requests for a particular domain are sent to the legitimate site or to a malicious site.

Figure 1 Sea Turtle attack process.



As part of the Sea Turtle attack, the DNS records for webmail servers were altered. This allowed the attacker to intercept connections from users logging into webmail systems, enabling the attacker to not only capture users' credentials, but also read all the data passed to and from the webmail system and the users.

DNS hijacking is an example of a non-direct attack, with the bad actors behind it wanting to disrupt the infrastructure of the Internet, rather than a specific organization.

At the end of this report, we explain how to fight cyberattacks like Sea Turtle, but there are some specific techniques to consider in preventing DNS misuse in the first place, such as monitoring passive DNS data and looking for changes to domain records in order to spot malicious changes.

Prognosis for 2020

The actors behind the "Sea Turtle" DNS hijacking campaign didn't slow down this year. In fact, Talos discovered new details that also suggest they regrouped after we published our initial findings about Sea Turtle and they redoubled their efforts with new infrastructure. While many actors will slow down once they are discovered, this group appears to be unusually brazen. Our advice in this instance is to place a particular focus on DNS security and multi-factor authentication for more rigorous identity verification.

Read more on DNS hijacking.

Source: https://blog.talosintelligence.com/2019/04/seaturtle.html

Noteworthy Mention: Targeted Ransomware

This year, there were a number of global high-profile instances of targeted ransomware attacks. Ransomware is of course nothing new, but it's important to state that while new forms of attack continue to appear, the old favorites never go away. The ransomware attacks described below demonstrate how destructive successful campaigns can be, especially when vital services are brought to a halt.

In May, the U.S. city of Baltimore suffered a massive ransomware attack that affected 7,000 users in city government buildings. The government refused to pay the ransom, but after resorting to entirely manual systems, and multiple data loss investigations, the event is estimated to have cost the city more than $10 million USD to recover.

Also in the U.S., Lake City, UT and Riviera Beach, FL suffered similar ransomware attacks, but chose to pay the hackers a combined $1 million in bitcoin. They still face the challenging work of decrypting the stolen data.

In the UK, Eurofins Scientific, a forensic firm used by police forces across the country, suffered a massive targeted ransomware attack. The firm deals with more than 70,000 criminal cases every year, and due to the scale of the cyber attack, a number of court cases were forced to be adjourned while other suppliers were found.

Read more on targeted ransomware, including a Talos discussion on how to deal with the ransom demand.

2. Remote Access Trojans (RATs)

The scenario

You're working for a high-profile technology company, close to releasing a market-changing product to the public. Your goal is to keep the secrets under wraps until the public announcement. Unfortunately, your surprise is about to be spoiled.

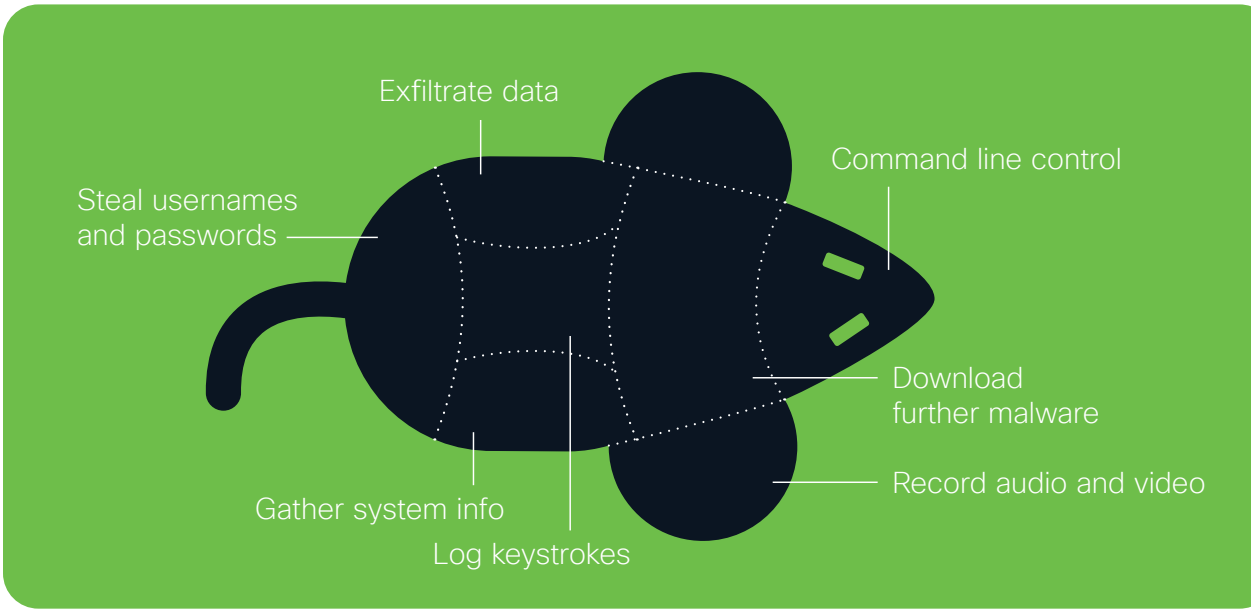
Someone has breached your company and stolen sensitive data about this new cornerstone product.

There may be a variety of useful weapons in an attacker's arsenal to steal intellectual property. Downloaders, administration tools, and info stealers often contribute to such an attack. But the go-to tool in scenarios like the one mentioned above is a remote access trojan, often referred to as a "RAT."

How a RAT can be used in an attack

As a tool, RATs provide a variety of capabilities. For example, if an attacker is hoping to exfiltrate financial data, they could leverage a RAT to scrape banking details from a compromised computer or collect credit card numbers by installing a keylogger.

Figure 2 Components of a RAT.



Many RATs include the ability to scrape saved and cached passwords, and once the usernames and passwords are in hand, the attacker can attempt to log in to the shared server.

The important thing to remember is that most RATs provide command line access to the systems that have been compromised. An attacker can use administrative rights to make a RAT do just about anything that he or she desires, such as installing and deleting files or installing a keylogger.

There isn't anything particularly special about the way a RAT gets onto a system. RATs are distributed in much the same way as other types of malware: they're sent by email, dropped by droppers, set up as the payloads for exploit kits, along with other common attack vectors.

Prognosis for 2020

It's perhaps a fitting coincidence that 2020 is "the year of the rat" according to the Chinese zodiac. Some recent RATs that have been prevalent on the threat landscape include Orcus RAT and RevengeRAT. In the summer of this year, Talos discovered a threat actor that had been leveraging RevengeRAT and Orcus RAT in various malware distribution campaigns targeting government entities, financial services organizations, information technology service providers, and consultancies.

They discovered several unique tactics, techniques, and procedures (TTPs) associated with these campaigns including:

- The use of persistence techniques most commonly associated with "fileless" malware
- Obfuscation techniques designed to mask C2 infrastructure
- Evasion designed to circumvent automated analysis platforms such as malware sandboxes

As cybercriminals look to extend the use cases for RATs, they certainly pose a threat in the year to come.

3. Threats in Encrypted Traffic

The scenario

Attackers go to great pains to get their threats onto systems and networks. And the last thing they want, after successfully penetrating an organization, is to have their traffic picked up by network monitoring tools. Many threats are now using encrypted traffic to prevent this from happening.

In terms of malicious functionality, there are a number of ways that threats use encryption. From command-and-control (C2) communications, to exfiltrating data, attackers consistently use encryption to hide their malicious traffic.

How to detect malicious encrypted traffic

One way to catch malicious encrypted traffic is through a technique called traffic fingerprinting. This involves monitoring the encrypted packets traveling across your network and looking for patterns that match known malicious activity.

However, this doesn't catch all malicious encrypted traffic, since bad actors can simply insert random or dummy packets into their traffic to mask the expected fingerprint. To identify malicious traffic in these cases, you need other detection techniques to identify the traffic, such as machine learning algorithms that can identify more complicated malicious connections. Threats may still manage to evade some machine learning detection methods, so implementing a layered approach and covering a wide variety of techniques is recommended.

Prognosis for 2020

Threats in encrypted traffic have been growing steadily. According to data gathered by Cisco, 63 percent of all threat incidents discovered by Cisco Stealthwatch were discovered in encrypted traffic. The industry is unlikely to turn back on the adoption of https, so it's crucial that organizations don't underestimate this as a tactic that some cybercriminals will try and be successful at leveraging. We look at the benefits of network analysis in our Conclusion section.

Read more on threats in encrypted traffic.

Figure 3 Banking trojans encrypt the data they're exfiltrating.

4. Office 365 Phishing

The scenario

You're in the midst of an email conversation with a colleague through your Office 365 accounts. You're chatting about a report you're ready to submit to the board, and your colleague sends you the final version.

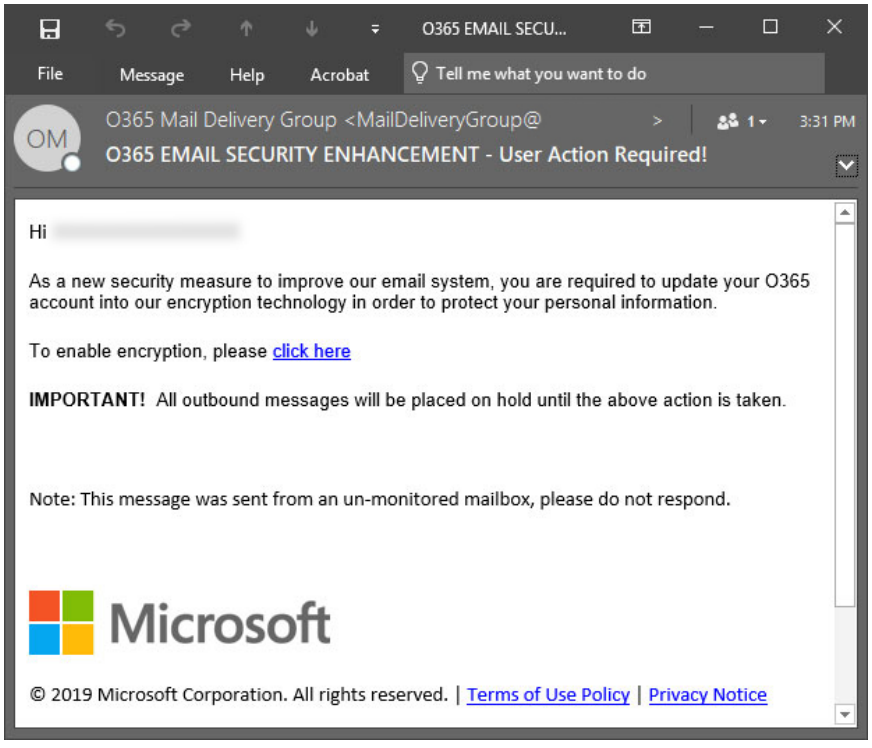
Except it's not your colleague. And that's not your report. Your conversation has been hijacked by a malicious intruder, who has compromised your organization's use of Office 365. Your emails to "colleague@yourcompany.com" were intercepted and replied to by the attacker, who tried to steer the conversation toward areas they wanted to find out more about.

The chain of events

The methods used by attackers to gain access to an Office 365 account are usually straightforward. The phishing campaigns typically take the form of an email seemingly from Microsoft. The email contains a request to log in, claiming perhaps that the user needs to reset their password, hasn't logged in recently, or that there's a problem with the account that needs their attention. The email includes a URL enticing the reader to click to remedy the issue.

In a successful Office 365 phish, the user enters their login credentials, which are scooped up by the attackers. The fake page does nothing, says that the login is incorrect, or redirects the user to the real Office 365 login page.

Figure 4 An sample Office 365 phishing email.



Given this series of events, most users would be none-the-wiser that their credentials had been stolen.

To make things more complicated, attackers often leverage "conversation hijacking," such as the scenario above, where they deliver their payload by replying to an email that's already located in the compromised inbox.

Prognosis for 2020

Based on a recent study conducted by ESG on behalf of Cisco, more than 80 percent of respondents reported that their organization is using SaaS email services like Office 365.[1] However, 43 percent of respondents still found that, after the move, they required secondary security technologies to shore up their email defenses.

Concern about user behavior (e.g., clicking malicious links in email or websites) remains high and is now the top concern for CISOs, according to our CISO Benchmark research. Only 51percent rate themselves as doing an excellent job of managing human resources on security via comprehensive employee onboarding and appropriate processes for handling employee transfers and departures. Additionally, in their 2019 Data Breach Investigations Report, Verizon reported that phishing had – by far – the highest success rate of any threat vector. During the last year, phishing was the primary weapon in almost a third (32%) of all data breaches.

Noteworthy Mention: Magecart Malware Returns

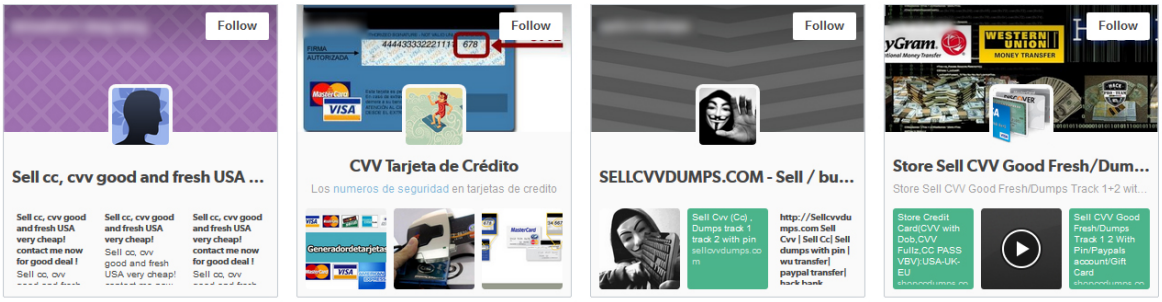
In 2019 we saw the return of the Magecart malware-website skimming malware that collects credit card details. Magecart was responsible for several high-profile data breaches in recent months, including flight booking and online ticketing services.

What's notable about its return this time is that it was used in several supply chain attacks. For example, in January we saw a supply chain attack hit hundreds of e-commerce sites that sold cosmetics, healthcare, and clothing products as well as the aforementioned industries.

The use of Magecart is significant in these attacks, as the attacker targeted third-party websites that these brands use for their e-commerce services, which allowed them to expand their reach and steal more data, rather than going after them individually.

1. Mark Bowker and Adam DeMattia, Solution Showcase: Cisco Email Security, ESG, October 2018.

Figure 5 Examples of attackers selling goods and services.



5. Social Media and Black Markets

You may think that cybercrime takes place in hidden corners of the Internet, utilizing heavily encrypted networks that require complicated software and extensive authorizations just to access. That's not always the case. Sometimes such activity takes place in very public places, such as social networks.

In the spring of 2019, researchers at Talos uncovered a vast collection of criminal groups with hundreds of thousands of members operating on Facebook out in the open. The groups were using the social media platform to connect with other criminals, share and sell tools, techniques and stolen data and, in some cases, to scam each other. Talos was able to establish – via extensive research and analysis – that some of the tools being shared via the Facebook groups could be connected to malicious activity from prior campaigns Talos has monitored.

An ongoing issue

It's important to note that cybercriminals haven't just discovered social networks as a vehicle to assist in their illicit activity. Some of the Facebook groups discovered have been around for as long as eight years as of this writing. Nor is this the first time that there's been a spotlight on their activity. In fact, security researcher Brian Krebs recently exposed 120 similar such groups with approximately 300,000 members. These groups were reportedly shut down, but that appears to have done little to deter those involved with such activities, judging by the number of groups Talos reported to Facebook in 2019.

Figure 6 Read more on the Talos investigations into social media and the black market.

The silver lining in this case is that users are not being targeted directly through this social media activity. The social media platforms are being used by criminals to discuss criminal operations. They're also being used as a marketplace to broker the purchasing of tools, including training on how to conduct attacks.

Prognosis for 2020

A quick search on Facebook at the end of 2019 for fairly obvious group names such as 'Spam professional' and 'Spam and hackers' revealed that these groups still exist, with several new posts every day. While we'll continue to report these groups to Facebook, as a security community, we can work together to report more.

6. Digital Extortion Scams

The scenario

You receive an email with the subject line containing both your username and password. Surprising as this would be, it's the body of the email that really gets your attention.

The sender claims to have compromised a pornographic website and that you had visited the site. The scammer says they took control of your monitor and webcam, recorded both you and the pornographic material, and then synched the two video streams together.

As if this wasn't disconcerting enough, the scammer claims to have gathered all of your contacts from your social media accounts and email. And finally, the scammer insinuates that it sure would be embarrassing if they were to send the video to these contacts.

Now the scammer claims that he isn't a monster and could easily erase this material. In fact, he is willing to make it all go away for the paltry sum of $1000 value in bitcoin.

The bluff

If this sounds like extortion, that's because it is. But it's also a bluff.

In this scenario, there's no truth to the email: no compromise of site, no control of webcam, no scraping of your contacts. He is playing on human emotions and guilty consciences. This is another series of phishing campaigns sent out in bulk, hoping to trick just enough recipients to make the scammer's efforts profitable. The inclusion of a genuine username and/or password makes the email seem more genuine. In fact, it's an attempt for scammers to make money from data stolen from previous breaches.

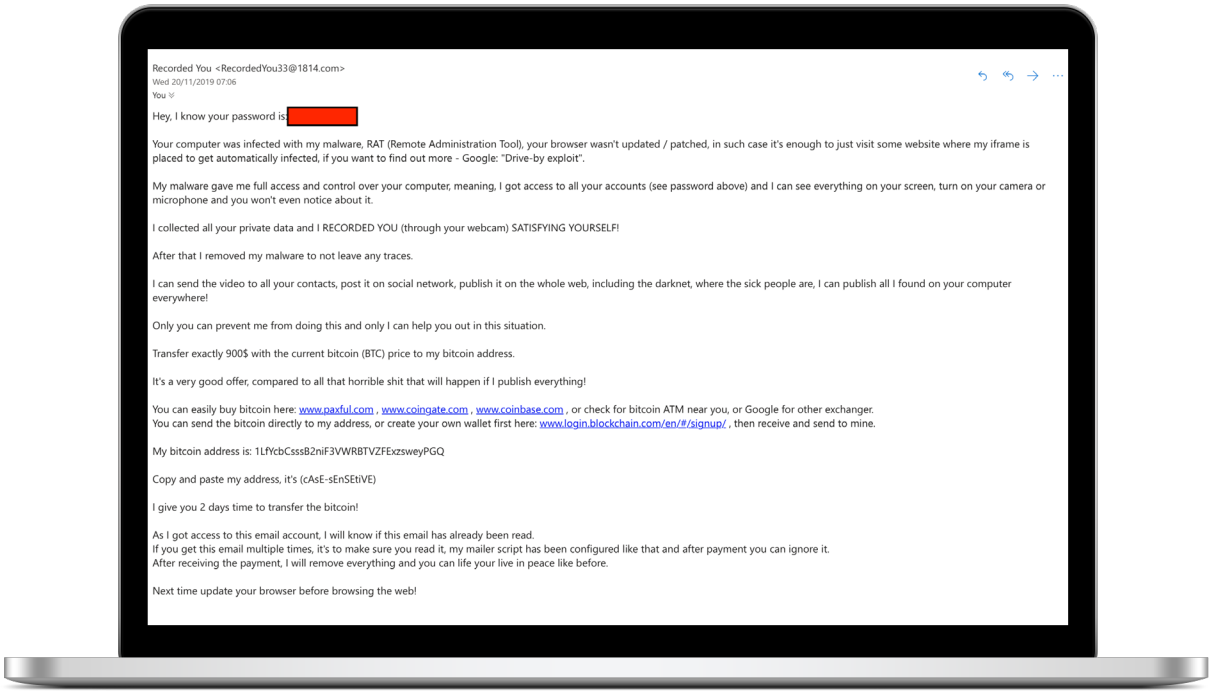
These emails are also full of more than their fair share of techno-babble. That's not to say it's impossible to view your Desktop or webcam remotely (it does happen), it's just highly improbable given the way the scammer describes it.

If you have received an email like this, understand that your personal data has likely just been obtained from a data breach. If you are still using that password elsewhere, change it immediately. If you're interested to find out if your email address has been exposed in a breach, check services like Have I Been Pwned, listing if and where this may have occurred.

Prognosis for 2020

Digital extortion attacks are still popular due to the small success rate needed to build profits. Figure 7 shows a recent example.

Figure 7 Recent example of a digital extortion email.



Methods to Combat These Threats

As with anything threat-related, a defense-in-depth security posture designed to address critical infrastructure will go a long way in protecting your organization.

Our #1 tip is to simply keep systems up to date and patch regularly. For example, in the case of Sea Turtle (the DNS hijacking case), attackers infiltrated systems by exploiting vulnerabilities, some of which were 10 years old.

Critical to that is to leverage threat intelligence as the backbone of your defense strategy. If you own a Cisco Security product, you're harnessing the power of Talos' threat intelligence, which flows to each and every one of our products.

Below is a list of solutions that form part of a layered defense, and a key for highlighting which threats each solution addresses.

Monitor DNS records and block malicious domains

Umbrella Investigate is a DNS inspection console that gives a complete view of the relationships and evolution of Internet domains, IPs, and files – helping to pinpoint attackers' infrastructures, predict future threats, and allow you to quickly find changes to DNS records. Being able to connect to C2 domains is also vital for many threats to function. Cisco Umbrella uses DNS to stop threats over all ports and protocols, even direct-to-IP connections, preventing connections to attackers' servers.

Threats protected against: DNS hijacking, RATs, targeted ransomware, threats in encrypted traffic

Employ a solid endpoint protection solution

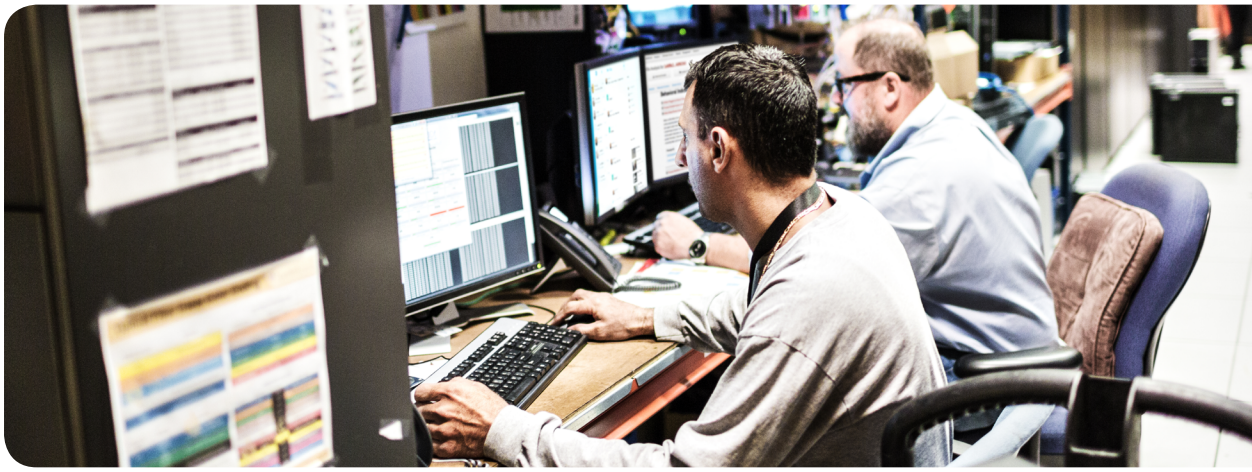
As more devices enter your network, it's crucial to understand what attacks are being leveraged at your endpoints, block them proactively, and respond rapidly to anything that breaches your defenses. Cisco AMP for Endpoints blocks malware at point of entry, then detects, contains, and remediates advanced threats.

Threats protected against: RATs

Use multi-factor authentication (MFA)

MFA solutions like Cisco Duo verify users' identities, gain visibility into every device, and enforce adaptive policies to secure access to every application. MFA can also prevent an attacker from logging into a system if they manage to obtain login credentials.

Threats protected against: RATs, targeted ransomware, DNS hijacking



Monitor network traffic

Monitoring for unauthorized activity is important. Cisco Stealthwatch is the most comprehensive visibility and network traffic security analytics solution that uses enterprise telemetry from the existing network infrastructure. Stealthwatch also includes Encrypted Traffic Analytics, which can find threats in encrypted traffic.

Threats protected against: RATs, threats in encrypted traffic

Email security

As well as the basics such as spam, virus, and malware prevention, consider more advanced phishing protections for email security that use machine learning to understand and authenticate email identities and behavioral relationships to block advanced phishing attacks.

Threats protected against: Office 365 phishing, RATs, digital extortion

Identify malicious file behavior

A solution like Cisco Threat Grid hunts for malicious files and automatically informs all Cisco Security products. Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

Threats protected against: Targeted ransomware, RATs

A platform approach

Holistically stop new infections, breach propagation and data exfiltration across multiple vectors and impacted systems with a platform approach such as Cisco Threat Response (CTR). The CTR platform automates and accelerates primary security operations functions: detection, investigation, and remediation. It is a key pillar of Cisco's integrated security architecture.

Threats protected against: All

Incident response

Strengthen your readiness and response to attacks. Talos Incident Response can help you prepare, respond, and recover from a breach by giving you direct access to the same threat intelligence available to Cisco. Our experts will work with you to evaluate existing plans, develop a new plan, and provide rapid assistance when you need it most.

About the Cisco Cybersecurity Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

In our new approach to thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise of threat researchers and innovators in the security industry, the reports in the 2019 series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others published throughout the year.

For more information, and to access all the reports and archived copies, visit www.cisco.com/go/securityreports.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published December 2019 THRT_08_1219