AVERTIUM

eBook

LOOKING BACK & MOVING FORWARD

An Overview of 2021 Cybersecurity Events & Predictions for 2022

TABLE OF CONTENTS

LOOKING BACK: 2021 TRENDS IN CYBERSECURITY

In 2021, we saw more than just advancements in technology and increases in ransomware attacks. The industry experienced new trends and changes in the standards for IT operations that altered our outlook on cybersecurity. From new methods of security implementation to government involvement, this truly has been a year of transformation for those working within the cybersecurity industry.

TREND #1

The Rise of Extended Detection + Response (XDR)

Extended Detection + Response (XDR) pairs an organization's existing and newly collected data with analytics tools, including machine learning algorithms, to do the heavy lifting of separating out benign activity, pointing out active threats, and automating protective responses. The term XDR was coined in 2018 and has become somewhat of a buzzword in the last year, sometimes sparking confusion around whether XDR is a tool, a process, or a service.

Analysts use advanced XDR technologies to comprehend how malicious activity spreads across attack surfaces - email, cloud, endpoint, and network - and what to do next. And remember… to an attacker, anything connected to the internet is part of a company's attack surface.

But why now, after almost four years, is XDR being noticed and trending in the industry?

1. **XDR enables CISOs to get a clearer picture and take proactive action.** XDR integrates tools and operations for a more complete view of your attack surface, which helps to proactively eliminate any areas of weakness within your security.

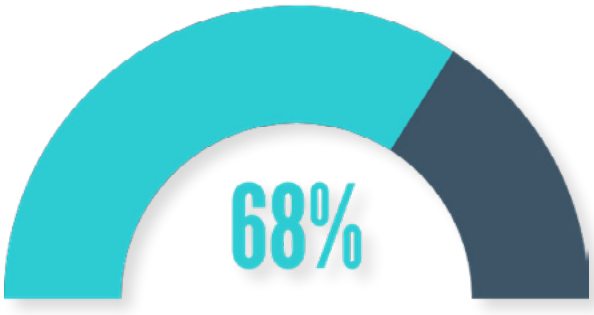
Related Content:

XDR: Tool, Process, Service, or all three?

2. **CISOs want to automate what they can within security operations.** XDR solutions can offer real value in improving security operations productivity with alert and incident correlation, as well as built-in automation. This enables more accurate and informed detection, higher SOC productivity, and faster time to remediation.

3. **XDR helps security professionals contextualize raw data.** Many XDR solutions reduce complexity through the logical convergence of multiple systems, particularly Security Incident and Event Management (SIEM) tools and MDR. This enables better visibility and searchability and therefore, faster time to value.

Throughout 2021, organizations implemented XDR into their cybersecurity strategy as it correlated differing tools for a better view of one's attack surface while only having to use one point of reference. So much so, that...



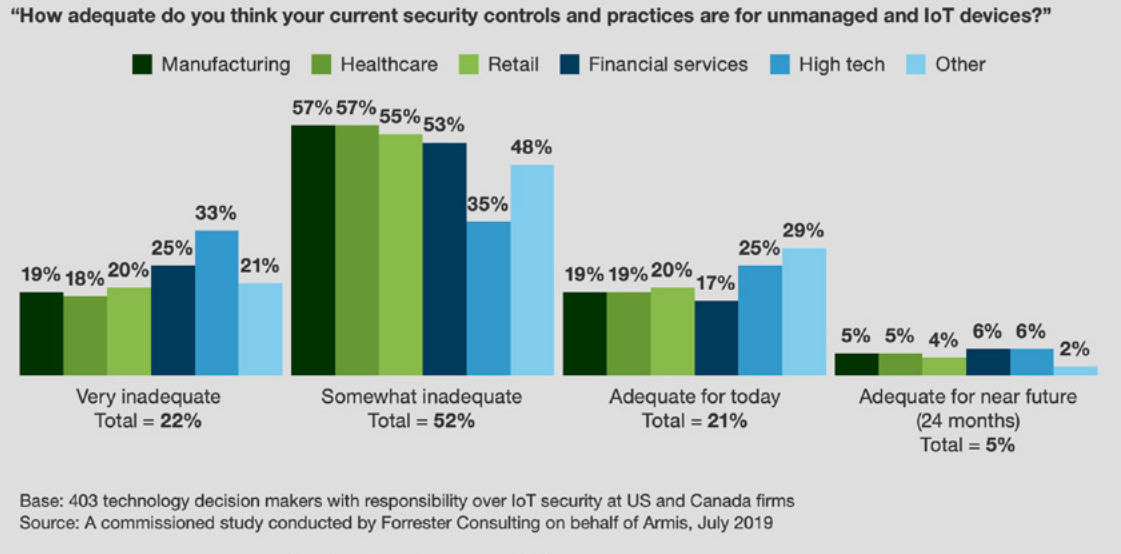
68% of organizations have implemented or plan to implement XDR in 2021 and 2022.

TREND #2

Changes in The Internet of Things (IoT) + The Rise of 5G Networks

The need for cybersecurity protection is no longer just about computers and cellphones. Every day, new technology is developed that acts as a channel for cyber threats to breach user data and spread throughout connected devices. From smart fridges to smart cars, from smart thermostats to tractor trailer efficiency monitors, wireless devices collecting data, sent back behind corporate firewalls are the real attack surface expansion worries to a corporation.

These could be backdoors into your environment… and they are often overlooked and undersecured.



Another major landmark shift in the cybersecurity and IoT landscape was the rise of 5G networks. 5G or 5th generation is the next step for technology and network connections.

According to Qualcomm, *"5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices."* While this advancement enables consumers with new benefits, it also provides new openings within your attack surface for cyber threats to utilize.

The combination of both expanding digital platforms, as well as the unfiltered connection provided by 5G, creates a perfect storm for hackers to infiltrate and spread throughout new devices.

Digital transformation is the greatest threat facing companies...

"The modern workplace and digital transformation alongside permeation of IoT across the enterprise [is the greatest threat facing companies]. The lack of a security-first mindset creates a significant weakness to businesses."

> Avertium Employee

TREND #3

Attacks at Home

A recent Comcast / Xfinity cybersecurity report suggested that xFi Advanced Security blocks an average of 104 security threats per month per household. **The top five most vulnerable devices in connected homes are:**

Computers & Laptops | Smart Phones | Networked Cameras | Networked Storage Devices | Streaming Video Devices

There is a consumer disconnect on cybersafe behavior:

- **The vast majority (85%) of respondents indicated they are taking all the necessary security precautions** needed to protect their home networks, and yet
- **64% admitted to behaviors** like sharing passwords with friends and family that open themselves up to attack.

TREND #4

The Shift in Data Storage

Throughout 2020 and 2021, the COVID-19 pandemic led to a universal migration of businesses to move online, increasing work-from-home (WFH) positions. This movement to WFH environments also called for organizations to shift their valuable information and data to off-site platforms such as cloud storage and personal computers (PCs). Within a short time span, companies drastically expanded their attack surface and ill-informed employees became easy targets for ransomware actors.

Today, with nearly 50% of worldwide corporate data being stowed away in cloud storage without regular or adequate backups, coupled with this move to work-from-home environments, cloud storage is a major threat.

Revenge of the rushed migration.

"The pressure of the business imperative to adopt cloud at rapid speed during the pandemic will begin to unravel as it becomes apparent security slipped through the cracks in rushed migration. As a result, we will witness the rise of huge breaches due to simple cloud security misconfigurations and permissions errors. This will fuel the mushrooming of startups based on automation of cloud configuration, permission analysis and remediation platforms."

> Archi Agarwal, founder and CEO of ThreatModeler

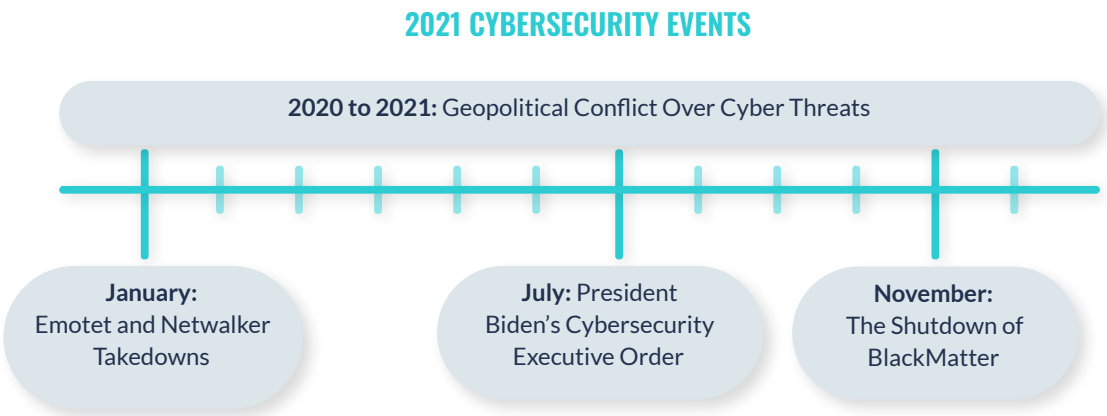
Related Content:

Ransomware Trends in 2021

TREND #5

Government Involvement in Cybersecurity

2021 included greater collaboration and information-sharing between the private and public sectors, as evidenced by significant cybersecurity events:



2020 to 2021 – Geopolitical Conflict Over Cyber Threats

Tensions are rising between different countries as cyber assaults have become a form of political attack. More specifically, Eastern European governments have put out an edict to target U.S. healthcare institutions earlier in 2020, painting an even bigger target on the backs of the U.S. Given that many ransomware gangs come from Eastern Europe, they often do not attack one another, and will also give refuge to cybercriminals by looking the other way.

January 2021 – Emotet and Netwalker Takedowns

Both Emotet and Netwalker are malware that infect your business in demand for a ransom payment. As of January 2021, the United States Department of Justice (DOJ) announced successful takedowns of Emotet and Netwalker, disrupting both strains of malware. Since the takedown, Emotet has re-emerged. Though the infrastructure takedowns are always only temporary, the cooperation and collaborative efforts between international governments to fight against ransomware transcends across borders.

July 2021 – President Biden's Cybersecurity Executive Order

President Biden administered an executive order aimed directly at tackling the cybersecurity challenges facing the United States. While this order mainly focused on the public sector, it did encourage information sharing between the private and public sector. In the end, it signaled a shift in the way that the US government is thinking about cybersecurity.

November 2021 – The Shutdown of BlackMatter

In November 2021, the ransomware group BlackMatter went public announcing their shutdown due to "pressure from authorities." It is believed that members of the group were being detained and held prisoner after the creation of an international law enforcement operation and therefore led to their collapse, though there is still speculation that they may re-emerge under a different name.

TREND #6

Cybersecurity Staffing Shortage

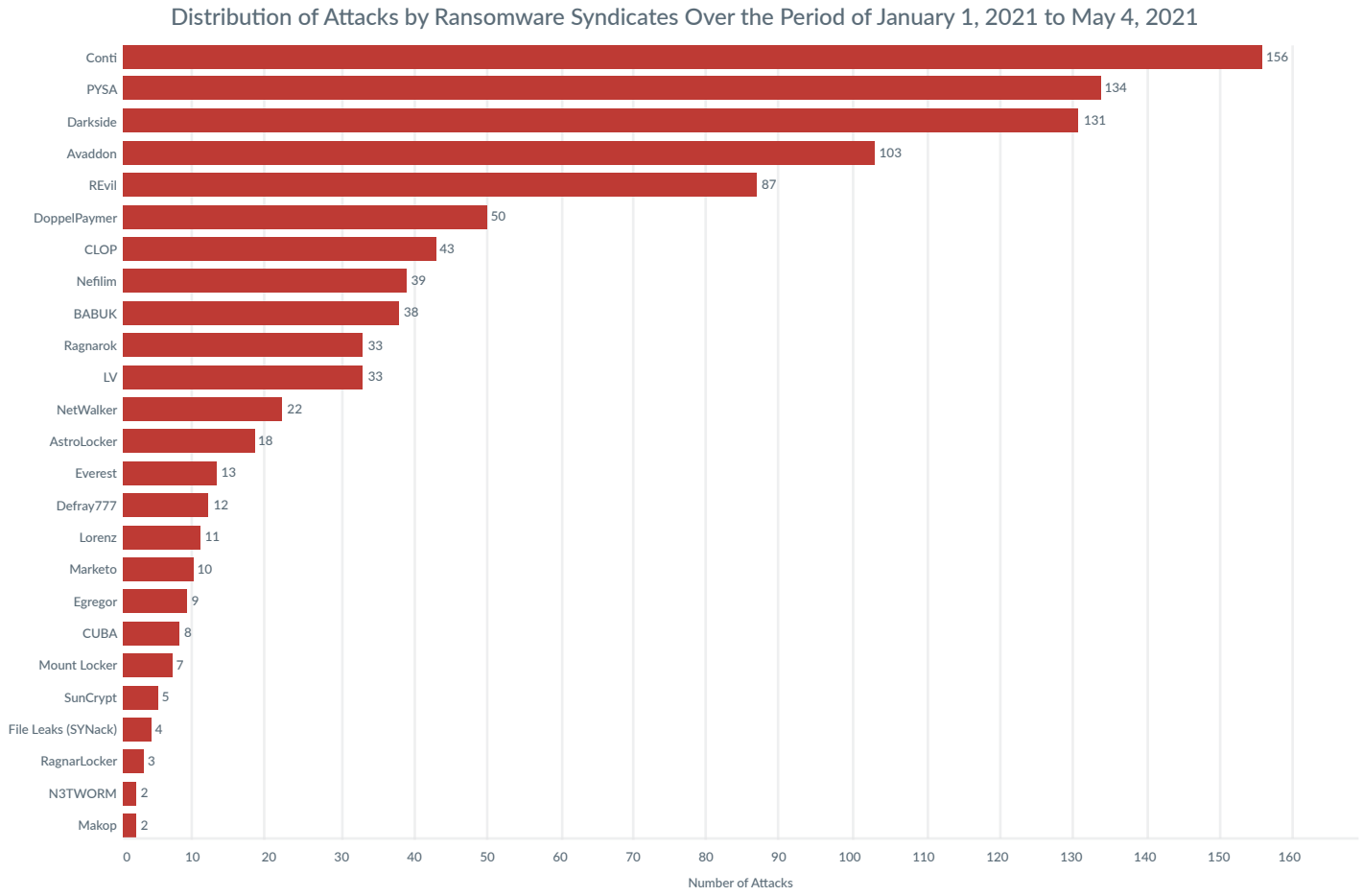
Though cybersecurity professionals have always been scarce and in-demand, 2021's global labor shortage made finding cybersecurity talent even more challenging for employers. At the beginning of this year, the Center for Strategic and International Studies found that there were 314,000 unfilled cyber positions within the U.S. government and predicted that it would reach 1.8 million globally by 2022.

Some of the consequences of this shortage are burnout and inexperienced talent being challenged against seasoned threat actors.

"The impact, especially this past year of the pandemic, has been significant. Teams are expected to do even more as a result of businesses moving to the remote operating model," says Candy Alexander, board president of ISSA International.

To combat this issue, the US government now offers free training courses and evaluations to encourage more people to explore the field. In the face of increasing desperation, organizations in the private sector have begun broadening their employment pool, hiring people with less experience.

THE YEAR OF RAAS GANGS



Source: AdvIntel Ransomtracker

It is important to note that paying the ransom does not always guarantee data recovery. The recovery statistics span the gamut. One source says 96% percent of victims receive the encryption key after paying the ransom, while another estimates that only 60% percent recover their data. Keep in mind, in some cases, paying the ransom and receiving the key does not guarantee that all data is recoverable.

Related Content:

RaaS gangs, Drive-By Downloads, and Botnets - Are You a Target?

LOOKING BACK AT 2021

MAJOR CYBER ATTACKS

The average total cost of a data breach within 2021 is at an all-time high. A report from IBM and the Ponemon Institute found that the average cost was $4.24 million USD PER INCIDENT … and this average goes up to $9.23 million per incident when the report limited its focus to industries that faced significant operational disruption during the pandemic such as health care, retail, hospitality, and manufacturing.

Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

Number of security incidents and breaches by victim industry and organization size

Source: Verizon Data Breach Statistics

It is important to note that not all attackers share the same intent when attempting to infiltrate a company's cybersecurity infrastructure. While a majority of threat actors seek to gain a profit, there are plenty of other groups who work to steal data with the purpose of disrupting national infrastructure, stealing intellectual property, or ruining an organization's brand image. And like a game of chess, we can stay three steps ahead of these threat actors by identifying their intent.

Knowing a hacker's objective allows us to group these breaches into specific categories: espionage, ransomware, and data leaks.

ESPIONAGE ATTACKS

United Nations Threat Recap

Who: *United Nations, Intergovernmental Organization*

When: April 2021

What Happened: Hackers broke into the United Nations' computer networks earlier this year, stealing a plethora of data that might be used to target UN institutions. The hackers' strategy for getting access to the UN network appears to be simple: they most likely used a stolen U.N. employee's username and password that they bought on the dark web. The credentials belonged to a project management account on the United Nations' proprietary platform. According to cybersecurity firm Resecurity, which identified the breach, the hackers were able to obtain further access to the UN's network from there.

The full scope of the breach has yet to be fully investigated as the UN continues to face new breaches periodically, each of which with the intent to obtain multi-national intelligence.

RANSOMWARE ATTACKS

Colonial Pipeline Ransomware Threat Recap

Who: *Colonial Pipeline, American Oil Pipeline System + Darkside Ransomware Group*

When: May 2021

What Happened: One of the most noted and discussed attacks of 2021 was the Colonial Pipeline shutdown. Behind the attack was the RaaS gang, DarkSide.

The U.S felt immediate impacts from the pipeline attack as the attack led to a supply chain disruption, causing the company to shut down much of the gasoline supply to the Eastern United States. To restore the network, DarkSide asked for a $5 million ransom.

But how did this happen? Entry into the company's network was suspected to be through a virtual private network (VPN) account. The VPN allowed employees

to remotely access the company's computer network. While the account was no longer being used when the attack happened, DarkSide was still able to access it. It was later discovered that the password for the account was revealed on the dark web, which means a Colonial Pipeline employee more than likely used the same password on another account that was previously hacked.

Additionally, the VPN account did not use multifactor authentication, which allowed DarkSide to breach the Colonial Pipeline network by using a stolen username and password. After several days, some ransom was paid and systems were restored, the crisis averted.

JBS Ransomware Threat Recap

Who: *JBS, Food Processing Organization + REvil and Sodinokibi Ransomware Groups*

When: June 2021

What Happened: JBS, the world's largest meat processing organization, was forced to pay $11 million after REvil infiltrated their network and shut down their plants within the U.S, Canada, and Australia. Leaked credentials in a remote location where the cybersecurity hygiene might have been at a different standard may have affected the rest of the global infrastructure.

It has been said that what is remarkable about this attack is how unremarkable it was in both execution and occurrence; it illustrates just how common ransomware attacks have become. Reconnaissance looking for vulnerable RDP Services were first sought out, but in the end, it appears several leaked credentials seemed to be the utilized attack vector.

Post attack, data exfiltration was observed from multiple sites several months prior to the ransom attack. It is estimated that 5TB or more of data was extracted prior to global sites being ransomed by the REvil / Sodinokibi group.

How REvil infiltrated JBS: JBS Meats discovered its information technology (IT) systems had been infiltrated by a ransomware attack on Sunday, May 30th. JBS Meats halted its North American and Australian computer systems in reaction to the attack, shutting down its beef processing operations in the United States, Australia, and Canada while significantly impacting operations at poultry and pork factories.

JBS reported late Tuesday, June 1, that it was starting to bring its systems back up, with the bulk of its systems expected to be operational by Wednesday, June 2. On June 2, the company stated that several of its pork, poultry, and prepared food operations in the United States, as well as a beef plant in Canada, were operational again. As the country recovers from the COVID outbreak, the attack has already affected the price of meat products, lowered cattle futures, and raised concerns about potential disruptions in food supply systems.

Source: AdvIntel, an Avertium Partner

Kaseya Ransomware Threat Recap

Who: *Kaseya, Software Company + REvil Ransomware Group*

When: July 2021

What Happened: The software company Kaseya was attacked by the ransomware group known as REvil. The breach led to a disastrous spread of ransomware that infiltrated 800-1,500 connected businesses worldwide.

This supply chain ransomware attack targeted many MSPs and their clients by exploiting a vulnerability in Kaseya VSA software. The attackers were able to bypass authentication controls, obtain access to an authenticated session, upload a malicious payload, and execute commands via SQL injection, resulting in code execution.

After infiltrating the VSA Server, any associated client will do what the VSA Server asks without inquiry. Kaseya was most likely targeted for this reason, and it basically worked against itself to spread the ransomware. The rest of the transaction has been well documented.

This is a major issue that has become common in breaches and is the reason why so many companies must be aware of the threat that their supply chains pose. As the months passedIn November of 2021, a Ukrainian national was found to be the culprit behind the attack, as he aimed to disrupt U.S infrastructure in November of 2021.

DATA BREACHES

Accenture Data Threat Recap

Who: *Accenture Consulting Firm + LockBit Ransomware Operators*

When: August 2021

What Happened: The attack on Accenture was one that proved to be the most costly. During Q3 2021, Global Consultancy Accenture was targeted by ransomware operators LockBit. The ransomware gang claimed to have exfiltrated over six terabytes of data (not confirmed) and demanded a $50 million ransom to be paid so that the stolen data would be kept private.

Accenture reported, *"During the fourth quarter of fiscal 2021, we identified irregular activity in one of our environments, which included the extraction of proprietary information by a third party, some of which was made available to the public by the third party."*

Accenture also notes that incidents such as unauthorized access to its systems, data theft, and breaches involving client systems enabled by or provided by the company have not had a material impact on operations, although a financial impact is expected.

Related Content:

July 4th Post Mortem on Printnightmare and REvil

As is now known, Accenture did not pay the requested amount in due time, the attackers published over 2,000 files allegedly stolen during the incident, threatening to publish more of them. It has been said by those on Twitter, who had reviewed the documents, that the files appear to be PowerPoints, case studies, quotes and the like. No PII appears to have been revealed.

After the main attack, Lockbit 2.0 spread malware throughout a multitude of Accenture's partner networks. This transmission of breaches to other organizations is another example of the importance of ensuring that your partners practice good cybersecurity hygiene.

T-Mobile Data Threat Recap

Who: *T-Mobile, Mobile Telecommunications + John Binns*

When: August 2021

What Happened: According to John Binns (AKA screen names including IRDev and v0rtex), the hacker behind the security breach, T-Mobile's security was "awful," allowing him to access the network with ease. He was able to steal thousands of customer's information including:

- SSN Numbers
- Names and Addresses
- Drivers License Numbers
- Dates of Birth
- IMEI (International Mobile Station Equipment Identity) and IMSI (International Mobile Subscriber Identity)Information

The stolen information was then later sold on the dark web and led to T-Mobile facing monetary loss as well as an ongoing public relations crisis.

Related Content:

You're Secure - But are Your Vendors?

INDIVIDUAL HACKER ATTACKS

More and more individuals are gaining knowledge of how to breach networks and the ability to pull off larger attacks with the assistance of RaaS gang tools. Examples of solo hackers from 2021 include:

- **John Binns –** As mentioned above, Binns infiltrated T-Mobile servers when he found an opening in their wireless data network that allowed access to two of their customer data centers. The breach was one of the most significant because of the number of records exposed and the regulatory repercussions to T-Mobile.

- **Alexsey Belan –** Alexsey has been active for more than a decade, gaining notoriety by hacking video game servers. By 2011, he was world-renowned. By 2012, he was wanted by the FBI. He went on to steal hundreds of millions of accounts from Yahoo and other sources, allegedly by request of the FSB (Federal Security Service of Russia).

- **Graham Ivan Clark –** Clark was responsible for hacking Twitter and asking for Bitcoin from Bill Gates, Elon Musk, Barack Obama, and maybe even Kanye. This event was all over the news, and with so many Twitter users, there was a lot of coverage. He could have received a ten-year sentence for his crimes but eventually pleaded out to a lesser term.

INTELLECTUAL PROPERTY THEFT

Sometimes it is not all about the ransom. Intellectual Property (IP) theft occurs much more often than it is actually publicized. You hear about the T-Mobile, Colonial Pipeline, and JBS Meat events… but with IP theft, bad actors want to be in/out before anyone knows what happened.

Businesses in the United States devote a large amount of money, resources, and time to developing highly useful products, technologies, and proprietary methodologies. Business competitors – and, increasingly, state actors or affiliates of state actors – are stealing that intellectual property at an alarming rate in order to gain an economic or national strategic advantage, with disastrous consequences for US business and national security.

In a story from the The National Interest, *The Wall Street Journal* published a story recently on Chinese courts declaring their firms cannot be sued anywhere in the world for theft of intellectual property, and in two cases threatening fines of $1 million per week if suits go forward. The US government is aware, but has done little. This is just one, recent event in decades of intellectual property (IP) theft and coercion by China and utter American failure to respond. In March 2021, the IP Commission confirmed that theft costs America hundreds of billions of dollars annually and the People's Republic of China (PRC) is the biggest culprit. It seems those original talks did not work. In 1995, the Clinton administration brokered an IP truce to avoid a $1 billion exchange of sanctions. Threaten $1 billion, then get to steal tens of billions annually — who says Beijing does not know a good investment when it sees it?

The US Government is looking into ways to negotiate with those states that are involved with this IP Theft, but the only real way to protect your business and IP is to greatly increase your cyber hygiene and awareness over those key assets.

LOOKING BACK AT 2021

WHAT WE LEARNED – KEY TAKEAWAYS

The three main takeaways that every organization should understand after 2021 and the cybersecurity events we have witnessed include:

1. **Anyone can be a target:** No matter the size or industry of your company, you are a target for ransomware and therefore should invest in cybersecurity to the best of your ability.

2. **Ransomware is adapting, and so should we:** Ransomware is adapting quickly to new methods of cybersecurity and consequently, we must adapt as well. The only way to beat a cyber threat is to prevent it, which means proactive threat hunting is becoming a must.

3. **You are reponsible for protecting the data:** If you are responsible for data that is not yours, then it is your job to protect it. Whether it be the log-in information of one of your company's partners or a client's phone number if you lose this information you will face more than financial repercussions.

LOOKING AHEAD: WHAT IS ON THE HORIZON FOR CYBERSECURITY IN 2022?

Heading into the new year, we are filled with uncertainty… but it is safe to say that cybersecurity in 2022 will be chaotic, evolving, and non-stop. Here are some of the predictions we have at Avertium:

CONTINUED RISE IN CYBER ATTACKS

We know it cannot be said enough - the fact is, the rise of ransomware attacks will not be slowing down anytime soon. Going into 2022, we can expect to see a continued increase in the frequency and scale of data breaches in every industry, targeting companies of all sizes. As organizations continue to expand their attack surfaces, so does the likelihood of unforeseeable and unprotected vulnerabilities.

The forces behind these increasing attacks include:

BotNets

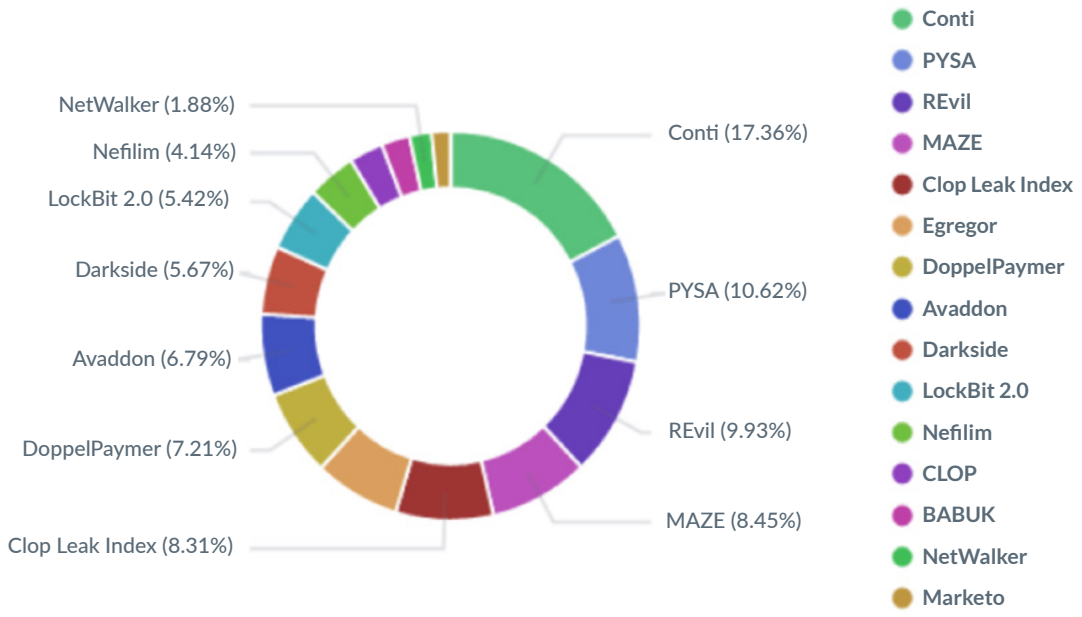
A botnet is a group of computers infected by malware that is under control of a single group or attacking party.

Andromeda botnet took the lead again in Q2 as the most witnessed botnet – consisting of 47.93% of all witnessed botnet activity. Torpig Mebroot also was prominent this quarter, finishing in second place and consisting of 22.02% of all witnessed activity in Q2. Notably, ZeroAccess dropped to the fifth most observed botnet in Q2, although ZeroAccess's activity has been known to come in waves.

Source: ANuspire, Q1 2021

RaaS (Ransomware as a Service) Gangs

RaaS and Botnets could be discussed together, as when they collaborate, they become even more efficient at infiltrating organizations. RaaS gangs "rent" software from the Administrator as the ransomware creators are sometimes called, so they get a cut of the proceeds when there is a victim. This makes it easier for the less sophisticated cybercriminals and gangs to proliferate ransomware and wreak havoc. When you combine these gangs with the efficiency of a Botnet's distribution system, you can see why these attacks are on the rise.



Source: AdvIntel Ransomtracker, 3,500 entities tracked since 2020

Lockbit 2.0 is certainly one to be cautious of, having recently added Accenture to their list of victims.

Since the second quarter of this year, the group has infiltrated more than 50 multinational companies. Researchers explain, *"All of the threat actors' posts on their leak site feature a countdown until sensitive information is released to the public, which adds to the victim's stress."*

LockBit 2.0 commences file encryption and appends the .lockbit extension when it is run. When the encryption is complete, a ransom note called Restore-My-Files.txt alerts victims of the breach and provides instructions on how to recover their files.

Encryption speed comparative table for some ransomware							
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460	random extension

Source: PaloAltoNetworks, partial table showing data encryption speeds C/O PAN, Unit42

As healthcare facilities hold highly sensitive personally identifiable information (PII) of patients, Hive often attempts to coerce the victim into paying more money than in a traditional ransomware attack.

Related Content:

Why the Time is Now for CISOs to Advocate for Cybersecurity

AN INCREASE OF CYBER THREATS IN HEALTHCARE

Between 2015 and 2019 alone, over 157 million patient records were exposed to data breaches. Here are some of the reasons why the industry can expect a continued increase in breach attempts for 2022:

- Pressure and distraction from the ongoing COVID-19 pandemic
- The growing amount of data and personal information that hospitals and other healthcare facilities store
- A lack of emphasis placed on cybersecurity within healthcare

The Hive RaaS gang, for example, seems to specifically target the healthcare segment in its attacks. In 2021, they notably targeted Memorial Health System hospitals in Ohio. Hive is a double-extortion ransomware group making revenue with a two-pronged attack that involves:

1. Stealing critical data
2. Locking down their victims' machines

A MIGRATION TOWARDS CYBERSECURITY INVESTMENT WITHIN THE PRIVATE SECTOR

According to Gartner, global IT and cybersecurity spending has been steadily increasing for both the public and private sectors. While the information security market was just under $124 billion in 2020, Gartner expects it to reach more than $170 billion by 2022. **This will include private organizations investing in:**

MSSPs (Managed Security Service Provider)

Off-the-shelf security tools

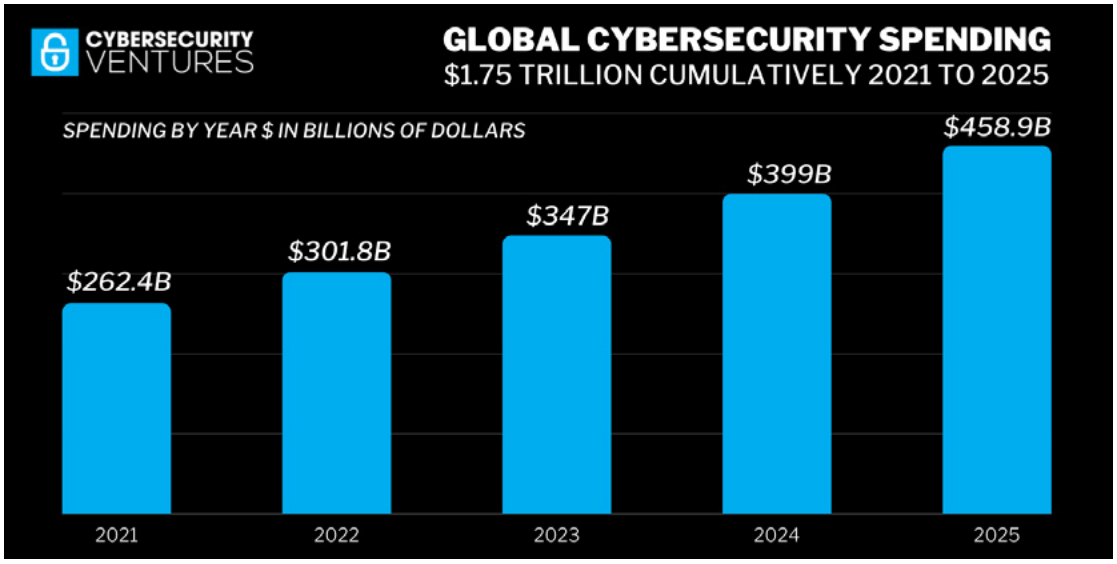
CISOs (Chief Information Security Officer)

It should also include* investing in technologies such as:

- Extended Detection + Response (XDR)
- Multi Factor Authentication
- Zero Trust Networking
- Network Segmentation

**not an exhaustive list*

Many larger organizations within the U.S have already begun to implement new standards of cybersecurity; however, it is smaller companies with an "it could never happen to me" mindset," that are just now beginning to understand the necessity for security and that they are just as much of a target as any other organization.



Source: Cybersecurity Ventures, Market Report

RETALIATION FROM THE GOVERNMENT ON CYBER ATTACKS

As mentioned previously, national governments began to take a more in-depth interest in cybersecurity this year, but we expect this to become a major concern for them in the near future as ransomware groups continue to grow and implement new tactics such as "Killware."

Killware is a form of malware intended to cause physical harm or death by infiltrating and disrupting vital national infrastructure. During a 2021 cyber-attack located in Florida, a water treatment facility was breached and the hacker increased levels of sodium hydroxide into the water supply with the intention of harming surrounding residents. This is believed to be the next phase in ransomware and therefore has forced the government to take action.

At least 45 states within the U.S. and Puerto Rico introduced/considered more than 250 bills and resolutions that deal significantly with cybersecurity. The federal trade commission is gaining a heavy influence on cybersecurity regulation as they are monitoring companies with low-security measures and enforcing action on them for better protection. Some of the states which enacted legislation for cybersecurity in the 2021include:

- Arkansas (AR S.B. 149) – Anyone licensed and working within the mortgage industry must have updated and established cybersecurity to protect client information.
- Colorado (CO H.B. 1236) – Allows the Cybersecurity Council of Colorado to create and enforce cybersecurity standards for both state and local governments.
- Florida (FL H.B. 1297) – The general inspector of Florida will now audit and advise cybersecurity measures within computer networks for the Department of Managed Services.

[This is] a situation we've not yet fully experienced.

"Ransomware remains the most crippling, while Killware has appeared recently in the news through a mention by the Department of Homeland Security. The latter opens the possibility of human casualties in direct association with a cyber-attack. A situation we've not yet fully experienced."

> Gary Monti, Director of Security Operations & Service Delivery Management at Avertium

HOW YOU CAN PREVENT RANSOMWARE & OPTIMIZE YOUR CYBERSECURITY

As we head into 2022, it is imperative to recognize that there is no industry or company that is not a target for cyber threats. Beyond that, there is no way to protect yourself with 100% certainty. That is the bad news.

The good news is that there are ways to create friction for attackers and that friction often forces those attackers to move onto easier targets. Companies that are more likely to experience breaches are the ones that do not regularly assess their vulnerabilities in preparation for an attack. Following these steps could be the building blocks to help you along the way to building more cybersecurity resilience.

TIP #1

Build a Human Firewall

Employees are targeted by dozens of phishing emails every day. One of the most effective ways to prevent & detect ransomware attacks is by educating employees through a phishing awareness training program. Disseminating current and relevant training and information provides employees with an understanding of these threats, what they look like in an email, and common paths hackers take to gain access.

While email scanning systems can help with weeding out many threats, training employees to detect the rest can dramatically decrease an organization's vulnerability to an attack.

TIP #2

Utilize Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) should always be used. Wherever practical, businesses should use multifactor authentication. MFA can mean the difference between a successful attack and access to your network being denied.

TIP #3

Keep Systems Updated

The majority of ransomware is spread through traditional ransomware methods, but there are exceptions. The famous WannaCry outbreak was spread by exploiting a vulnerability in Server Message Block (SMB), a common protocol Windows uses to share files, printers, and serial ports on the same network or domain.

The attack could have been entirely prevented if organizations had updated their systems with patches addressing the vulnerability - patches that were available months earlier. As a security best practice, promptly installing necessary system patches will considerably reduce the likelihood of a security breach. Threat actors are fast to exploit new flaws with the aim of outwitting system administrators and getting access to unprotected systems. Check the security alerts from your vendors and follow their patching/mitigation procedures.

TIP #4

Monitoring, Detection, & Prevention

Ransomware acts quickly. For it to be effective, it needs to be able to open, encrypt, and delete many files on a computer before you can do anything about it. Cybercriminals do their homework, observing and researching the best ways to attack.

This suspicious or unusual user behavior makes it possible to detect and shut down a ransomware attack if the organization reacts quickly. Having tools in place to configure endpoint detection systems to generate alerts based on relevant indicators, alongside an adequate quarantine plan, can go a long way in stopping the spread of a possible infection.

Related Content:

Understanding Cybersecurity Best Practices

TIP #5

Limit User Privileges

A ransomware infection can only encrypt files that it can access. If most users operate with administrator-level access by default, this means the infection can encrypt all of them.

In general, most employees do not need administrator-level permissions on their work machines. While it is often necessary for installing software, it is not needed for editing documents and checking emails. By limiting permissions to the minimum necessary and setting up a process for handling exceptions, the impact of a ransomware infection can be minimized.

TIP #6

Deploy an Automated Backup System

The revenue model of ransomware depends on its targets being desperate enough to pay large sums of money to hackers to get their data back. If this is not the case, the whole system falls apart.

Deploying an automated backup system can help limit the impact of a ransomware attack. The value of an hour (or less) of lost data is often far less than the ransom being demanded by an attacker. By deploying an automated backup system that is ransomware resistant, an organization can minimize the impact of an attack.

Cloud service providers introduce new supply chain risks.

"Every cloud provider should be thinking about supply chain risks and vulnerabilities (i.e. user permissions, cloud misconfigurations). There are areas of risk in the lower level of cloud services, that if not secured properly, could lead to a massive infrastructure attack, something in scale that we've not seen before. Organizations must be prepared for this."

> Jeff Costlow, Chief Information Security Officer at ExtraHop

TIP #7

Attack Chaos with Context Using Open XDR

Evasive threats are becoming more common every day, making it more difficult for the old methods of detection to keep up. Significant technology advances in Endpoint Detection and Response (EDR)* have made it faster and easier than ever for security teams to stop potential threats in their tracks. Not only has EDR made significant advancements, but System Information and Event Management (SIEM)* technologies have also come a long way. Today, SIEMs are integral parts of comprehensive cybersecurity solutions, going beyond basic log management to help with advanced threat detection and response, alongside regulatory and compliance reporting, for many organizations.

With that said, cyber threats are becoming more sophisticated, **standalone EDR and SIEM solutions are no longer enough** to protect your business from the storm of cyber-attacks. The Show No Weakness approach means you need context – a unified view of context amongst the sea of signals, tools, and telemetry. **That is what Extended Detection and Response (XDR) technology is all about.**

XDR technology piqued people's interest in 2021, and it is clear that popularity will **continue to grow** as we move through 2022.

Avertium's A^{v}XDR takes XDR technology and adds a NIST CSF, alongside Attack Surface Management (ASM) technology and Cyber Threat Intelligence (CTI), to deliver a truly integrated, strategic solution – **one that connects and contextualizes your data to enable swift detection and rapid response**.

**Avertium Technology Partners: SentinelOne EDR, LogRhythm SIEM, and Microsoft SIEM*

Related Contents:

XDR is Not Only About Technology and Why this Matters

Building an XDR Solution: Factors You Ought to Consider for ZTNA, EDR, Vulnerability Scanning and SIEM

AND FINALLY,

Strengthen Your Cybersecurity in 2022 with Avertium

As we approach 2022, enhancing your company's cybersecurity resilience can no longer stay at the bottom of your to-do list.

The cybersecurity landscape is pure chaos, and Avertium plays an important role in bringing context to that chaos.

1. **Business-First Mindset** With tactical information in the context of a bigger picture approach, you can quickly and efficiently improve security posture without compromising coverage, existing technology investment, or business continuity - all while building a more resilient, more measurable security program that scales alongside your business and the threat landscape.

2. **Cyber Fusion Philosophy** We can help you bring together disparate data sources and put it in the context of your threat environment, the threat landscape, and your available resources. With this context, you can see every threat, extend your reach, adapt, attack, and evolve with context.

3. **Human Element** The latest and greatest technology is great, but it is often not enough. In the cyber war, you are not fighting technology… you are fighting humans. That is why Avertium puts humans at the forefront of technology, bringing superior teaming at both a tactical and strategic level, alongside deep capabilities in every cybersecurity specialty from monitoring and detection to training and compliance, plus the commitment to work collaboratively with every single client.

There is no technological solution to security...

"There is no technological solution to security, you need to have the right people and cybersecurity needs to be embedded throughout all of your systems."

> Avertium Employee

CONCLUSION

THE STATE OF CYBERSECURITY IN 2021 & LOOKING AHEAD TO 2022

We can expect the same as we look ahead in 2022.

While ransomware continues to proliferate and the RaaS Gangs continue to hunt for targets, **we must remember that staying proactive is our best defense**. Fortunately, in an effort to strengthen cyber defense measures, both law enforcement and intelligence agencies are making cybersecurity a priority (even in non-cooperating countries).

And though the future remains uncertain, we can use the past as insight for what is to come.

ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why **over 1,200** mid-market and enterprise-level organizations **across 15 industries** turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

CONNECT WITH US

AVERTIUM

Cyber Fusion Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

SHOW NO WEAKNESS®