Protecting Against Ransomware

Zero Trust Security For a Modern Workforce

Table of Contents

Ransomware is here to stay

Ransomware has evolved quickly as an attack strategy. Once a hostile takeover of lone computers, today the stakes are rising. Bad actors increasingly take aim at geopolitical targets, critical business systems and infrastructures (e.g., big game hunting), which could result in unprecedented damage. Today, ransomware is one of the biggest threats in cybersecurity, increasing by 150% in 2020 due to the sudden shift to remote work.

Ransomware is now classified as cyber terrorism, and the recent executive order from U.S. President Biden confirms that action must be taken now to keep systems safe. A zero trust approach is the gold standard to protect against ransomware. The National Institute of Standards and Technology (NIST) says, “implementing a zero trust architecture has become a cybersecurity mandate and a business imperative.”

The White House fact sheet states, “Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals.”

> “Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals.”

Fact Sheet from The White House of the United States of America.

What is Ransomware?

Simply put, ransomware uses a variety of tactics to target users predominately through malware infections, usually beginning with email phishing, a stolen password or a brute force attack. A ransomware attack can be achieved by encrypting files or folders, preventing system access to the hard drive, and manipulating the master boot record to interrupt the system's boot process. Once the malware has been installed and spread, hackers can gain access to sensitive data and backup data, which they encrypt in order to hold the information hostage. Hackers can move quickly or spend months poking around undetected to understand the network infrastructure before launching an attack.

The data hijack is meant to elicit fear and urgency from victims. Their information is inaccessible until payment (primarily in Bitcoin) can be made. Even then, companies may not get back all of their data. There are many ransomware variants, but for the most part, cryptoransomware dominates the field. Due to polymorphism (malware that constantly changes), there are many variants that can avoid detection.

The cryptoransomware that locks data is improving quickly. In 2006, ransomware used 56 bits with homemade encryption. Today's advanced version of ransomware uses AES symmetric algorithms and RSA or ECC public-key encryption to block data.

Ransomware matures into a business

As ransomware continues to gain momentum, it has matured into a professional business run by criminal organizations (mostly located in China, Russia, North Korea and Eastern Europe) dedicated to marking and disrupting high-value targets and extracting money in exchange for data. To do this effectively, these organizations have even gone so far as to set up call centers to walk targets through the process of buying Bitcoin and paying the ransom. Some are even highly rated for good customer service by their targets.

Sometimes to incentivize payment, attackers will provide a play-by-play "security report" that details exactly how they conducted the attack after the exchange for the ransom. While it would be smart for gangs to decrypt the files in exchange for money to keep their reputation intact for the next target, that's not always the case. Sophos' The State of Ransomware 2021 states that only 8% of victims get their data back and 29% recover more than half of it back. Sometimes the data is harvested and traded to other attackers or held for another future ransom opportunity.

In recent years, bad actors have established ransomware-as-a-service (RaaS), a fully integrated out-of-the-box solution allowing anyone to deploy a ransomware attack without knowing how to code. Just like Software-as-a-Service (SaaS) products, RaaS gives relatively cheap and easy access to these types of malicious programs for a fee smaller than the cost of creating your own. RaaS providers generally take a 20%-30% cut of the ransom profit generated. There are now subscription and affiliate models to help complete successful attacks. The hacker group REvil had an affiliate model that would profit share with anyone who contributes to a successful ransomware attack. This model has led to the dramatic increase in the volume of ransomware attacks.

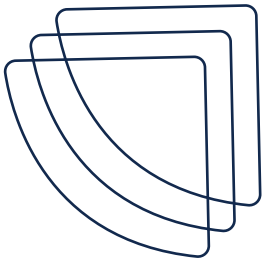
First attributed to the Maze gang, another trend is double extortion, in which the hackers take the hijacked information and threaten to publish it on the dark web and/or internet if their demands are not met. They have built-in infrastructure to handle these data dumps, according to Verizon's 2020 Data Breach Investigations Report. The "name and shame" tactic is now popular for most ransomware gangs, as is the "penalty" model, where the price increases as more time passes.

As companies harden their security posture for computers and networks from ransomware attacks, the hackers are now turning their attention to exploiting mobile devices. Mobile devices have a much smaller screen and do not provide complete information at first glance (email as an example), making it easier for victims to click on malicious links. Internet of things (IoT) attacks are also on the rise, as ransomware and lack of security can turn devices and objects into entry points for ransomware tools. In 2020, ransomware attacks targeting IoT devices increased 109% throughout the U.S.

These factors, coupled with countries that act as safe havens for attackers, have led to the rise in ransomware crime. There was a successful ransomware attack every 10 seconds in 2020, and according to a Anomali Harris Poll survey one in five Americans are victims of ransomware attacks. Furthermore, Infosecurity Magazine reports the most popular method of attack "by far was botnet traffic (28%), followed by cryptominers (21%), information stealers (16%), mobile (15%) and banking malware (14%)." In response, companies are scrambling to spend more money on security ($150 billion in 2021 according too Gartner).

Attacks on individuals are declining as hackers focus on more lucrative specific targets. Managed service providers (MSPs) are reporting an 85% rise in attacks against SMBs. Enterprises, along with infrastructure, healthcare, government and manufacturing companies are being targeted more than ever before, with price tags in the millions in exchange for their data. The size for a ransom has doubled in the past year as attackers hit bigger companies. Attacks on vendors, contractors and third-party software have also steeply increased. Companies have had to rely on the security of these outside parties who have access to their systems.

The rise of ransomware gangs	The first known instance of ransomware came from floppy discs that contained AIDS surveys and malware, distributed all over the world in 1989 by Dr. Joseph Popp. The discs would encrypt files on the victim's system and deny access until they sent a $189 payment to a post office box in Panama. Bait CDs were then distributed at the World Health Organization's AIDS conference. Payment and shipping CDs was problematic and expensive.
2006	Cybercriminals began using a more effective form of 660 RSA public key encryp-tion to encrypt files faster. Big players in that era were the Archiveus Trojan and the GPcode that used phishing email as their entry points.
2008-2009	New antivirus software loaded with ransomware malware appeared, and rogue security software used FileFix Pro to extort money for decryption.
2010	Bitcoin changed everything. Ten thousand ransomware variants were detected, and screen locking ransomware made its first appearance.
2013	A quarter of a million samples of ransomware existed, and Cryptolocker and Bitcoin quickly became the primary payment method. Ransomware used 2048-bit RSA encryption for increased demands, proving lucrative for gangs.
2015	The Teslacrypt ransomware trojan appeared, there were now 4 million variants of ransomware, and ransomware-as-a-service (RaaS) was introduced.
2016	JavaScript and Locky ransomware was popular, with Locky infecting 90,000 vic-tims per day. Attackers targeted larger organizations, like hospitals and academic institutions. Ransomware reached more than $1 billion in profits. Petya malware caused over $10 billion in financial losses.
2017	The WannaCry cryptoworm appeared this year, evolving into a variety of variants daily and quickly spreading to 300,000 computers worldwide through a Mi-crosoft exploit.
2018	Katsuya was introduced. SamSam shut down multiple municipal services impacting the city of Atlanta.
2019	REvil, a private RaaS gang, emerged from Russia. Ryuk, a sophisticated and costly ransomware variant which embedded in malicious attachments and phishing emails, demanded higher payments compared to similar attacks and effectively shut down all of the major newspapers in the U.S.
2020	Darkside, Egregor and Sodinokibi rose as major players. Ryuk went from one case a day to 19.9 million by September, the equivalent to eight cases per second.
2021	REvil/Sodinokibi, Conti and Lockbit kits hit healthcare hard. CryptoLocker squeezed $40 million from major insurance provider CNA Financial in one of the largest ransomware payments to date. The DarkSide succeeded in attacking the Colonial Pipeline Company, marking the largest publicly disclosed hack of U.S. critical infrastructure.



The perimeter expands

How did ransomware become so prevalent? Previously, the perimeter was a gated wall that managed centralized data and applications through virtual private network (VPN) firewalls and Mobile Device Management (MDM) solutions, like a moat surrounding the network castle. Today, work happens from anywhere and any device (including personal mobile devices), and data needs to be accessed from third-party applications in the cloud. There is no moat, but rather many entrances to the castle. The surge of remote work during the pandemic turned the traditional perimeter into the “software-defined perimeter.” In the rush to keep employees working, security was an afterthought for many, which has led to ransomware opportunities for bad actors.

Remote access

Gartner Top Security and Risk Trends for 2021 reports that 64% of employees are now able to work from home, and two-fifths of the workforce are working from home. During the pandemic’s mandatory stay-at-home orders, the majority of workers had to go 100% remote and needed the ability to work on their own devices while accessing SaaS applications in the cloud and on-premises. Many companies did not have the infrastructure to support this change. Today, remote access is the new reality for the workforce. As organizations adapt to this standard of operating, it is predicted that the workforce will be a hybrid model of remote workers and those returning to the office.

Peter Firstbrook, VP Analyst at Gartner, said in a blog post, “As the new normal takes shape, all organizations will need an always-connected defensive posture, and clarity on what business risks remote users elevate to remain secure.”

Companies that have not strengthened their security posture for this change or fortified their internal security education create an easy way in for attackers. Gartner reports that 57% of breaches involve employee/third-party negligence. According to ZDNet, Remote Desktop Protocol (RDP) is the number one way that threat actors gain access to Windows computers and install ransomware and other malware, followed by email phishing and VPN bug exploits.

VPN constraints

Hacking exploits in VPNs is the third most popular method of entry for ransomware hackers. The hack that shut down the Colonial Pipeline Company was the result of one compromised password from an unused VPN. While VPNs can limit access to on-premises applications, there is inconsistency on accessing cloud applications which can lead to vulnerabilities. Once compromised, VPNs can lead to backdoor access to the network where hackers can install malware on internal systems.

A zero trust layered VPN and firewall approach with MFA prevents 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks, according to Google research.

Unprotected endpoints

As more and more devices connect to corporate networks, the number of personal devices and shadow devices have increased. Because these devices may not be monitored or up-to-date, they can potentially lead to breaches at key endpoints without being detected. As hackers meticulously look for a way in, unprotected endpoints and lack of insight on who and what is connecting to your network and the health of the device can lead to a breach.

Phishing, targeted attacks and vulnerabilities

Which techniques are used in ransomware attacks? It is a multi-step process that can be relatively short, or conducted over months to access and encrypt the data that is most valuable and will cause the most harm if held hostage. CSOonline.com reports that 94% of malware is delivered via email, and phishing attacks account for more than 80% of security incidents. Other entry points include unpatched updates and zero day vulnerabilities. Almost all of these begin by stealing credentials.

Ransomware techniques

Spray and Pray, or Broad-Based Phishing

Threat agents acquire email lists from the black market, then analyze the credentials and distribute phishing emails. Only a few credentials are necessary to be successful, often acquired via email with malicious attachments, fraudulent websites that appear legitimate, or a fake identity targeting high-value employees.

Spear phishing

This coordinated, targeted attack on a specific group of users is conducted by sending personalized, socially engineered messages invoking curiosity, fear or reward from a legitimate-looking source. The emails and website contain malware used to steal credentials. Malware can also be spread through social media and instant messaging applications.

Brute force

According to a LastPass survey, 91% of respondents acknowledged they reuse passwords. Hackers are well aware of this and collect passwords from credential dumps or the dark web. They then use automated tools to test passwords across different sites, known as credential stuffing or brute force. Once in, the attack can begin.

Exploiting known vulnerabilities

In addition to insight on what devices are connecting to your network, knowing device health and how current it is on patches and updates is important for maintaining a high security profile. Security Boulevard reports, “Outdated and ‘abandoned’ open source components are pervasive. And 91% of codebases contained components that either were more than four years out of date or had no development activity in the past two years.”

Step-by-step guide to a Ransomware Attack

Encrypting Ransomware	Coordinating the attack	Vertical movement
Most commonly, ransomware attacks encrypt data on the target systems, making them inaccessible until a ransom is paid for decryption. The latest tactic is double encryption, in which the hackers encrypt a system twice, or two different gangs target the same victim. With this approach, attackers have a chance to collect two ransoms by receiving payment for the first layer of encryption, and then surprising victims with another layer after collecting payment for the first. The most common encryption is asymmetric or symmetric.	At this point, ransomware hackers do their homework on the specific companies they're targeting. They might buy email lists from the dark web, identify important leaders, read up on the company's financials, research social media profiles, and compile a list of key stakeholders like contractors, vendors and partners. What tactics do hackers use to get in? The top three attacks in 2020 came from poorly secured RDP endpoints, email phishing attacks, and the exploitation of zero-day VPN vulnerabilities. Compromised credentials are the number one way bad actors gain access.	In the phase of infiltration and infection, vertical movement is when the threat actors move from an external position to an internal position. Once inside, they scan files and execute malicious code to endpoints and network devices. The malware moves through the infected system, disabling firewalls and antivirus software. By now, attackers have taken over the data, but it isn't encrypted yet. Common entry points for vertical movement include phished email accounts, low-level web servers, and poorly protected endpoints.

Lateral foothold	Exfiltrate the data	Payment and unlocking
Advanced persistent threats (APTs) have increased in success due to lateral movement. To establish a foothold, the criminals have to encrypt computers and spread the ransomware to as many systems as possible. Once access is gained, the hacker hunt begins. They begin to move laterally, undetected, for weeks or months through the network to identify key targets like the command and control center (C2), asymmetric keys and backup files. At the same time, they elevate their access and permissions by infecting additional systems and user accounts and prepare a persistent malicious presence to hijack data. Some examples of lateral movement include exploiting remote services, internal spear phishing, and using stolen passwords, also known as "pass the hash."	Once the inventory assessment is complete, the encryption begins. System backups are deleted, local files and folders are corrupted, unmapped network drives are connected to infected systems, and communication to the command and control center is made to generate the cryptographic keys used on the local system. The network data is copied locally, encrypted and then uploaded, replacing the original data. Exfiltrated data can be used to double extort. In this case, a ransom is demanded to decrypt the encrypted data, and then a second ransom is demanded not to leak the stolen data.	The attackers then activate the malware, block data, and announce their demands for a ransom at compromised locations with specific instructions on how to make the payment, typically to be paid in bitcoin. A ransomware hit creates a very expensive downtime problem that is extremely challenging to solve. Threats are made, and the countdown begins. Companies must decide whether they want to take the hit and pay, try to restore their files on their own, or use their cybersecurity insurance, which will only recover a portion of the ransom. It's a choice among bad options, which is why it's imperative that organizations implement a zero trust architecture and have hardened security best practices in place to avoid this situation.

Vulnerable industries

Healthcare, municipalities and government, as well as retail, education and finance, are the industries most impacted by ransomware hits. These industries have complex legacy solutions and may not leverage robust cloud security. Healthcare, education and government are slow to adapt their security posture with updates and new technology, making them lucrative, easy targets.

Stopping Ransomware compromise before it starts

In a ransomware attack, attackers first need to gain access. They can do so by obtaining compromised credentials, as was the case in the Colonial Pipeline breach.

Duo Multi-Factor Authentication (MFA) can help prevent ransomware from gaining access in the first place. MFA requires a user to present a combination of two or more credentials to verify their identity for login. For example, in addition to a username and password, Duo MFA asks for something you have – like a trusted device, or a software or hardware token – before granting access to resources. Thanks to this additional requirement, MFA makes it a lot more challenging for ransomware to get that initial foothold.

Ransomware is also keen on using remote services, such as RDP and VPNs, to gain access to a network. Darkside, the alleged perpetrator of the Colonial Pipeline attack, is suspected to have used corporate VPN access to gain entry into the victim's environment. More than just MFA, Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) and Duo Trust Monitor combine into one trusted access solution and can help secure remote access to on-premises infrastructure and prevent ransomware from getting access in the first place.

Duo MFA requires more than a username and password to authenticate. DNG allows users to access on-premises websites, web applications, SSH servers and RDP without having to worry about VPN credentials. Duo Device Trust ensures that the device remotely accessing resources is a trusted computer and not an attacker's device. Finally, Duo Trust Monitor brings attention to authentication requests that appear suspicious, such as originating from countries where ransomware actors are known to be active, and countries where an organization does not have employees.

The use of malware is also a popular ransomware infection technique. Cisco provides additional complementary solutions, such as Secure Endpoint and Email Gateway, that can inspect, detect and block malware-based ransomware before it infects endpoints.

How Duo helps protect against Ransomware

Gartner reports 90% of ransomware is preventable. Duo is uniquely positioned to help organizations on three fronts:

1. Preventing ransomware from getting an initial foothold in an environment
2. Preventing or slowing down the propagation of ransomware if it manages to infiltrate an organization
3. Protecting critical assets and parts of the organization while an attacker still has a presence in the environment and until full remediation is achieved

Fending off the propagation

Ransomware that affects a small number of systems has a limited impact and is unlikely to cause an organization to grind to a halt and want to pay a ransom. This is why propagation of ransomware is crucial to effectively bringing down a significant portion of an organization and compel them to pay the ransom to quickly get back to business. Back in 2017, WannaCry and NotPetya used the External Blue exploit to take advantage of a Microsoft vulnerability and spread it without user intervention.

Duo's Device Health Application can keep devices patched and up-to-date, making it harder for ransomware to spread automatically. In addition, it provides visibility while checking the device health status, including how updated the device is, at every single login attempt. And with Duo's self-remediation capability, users can easily keep their devices patched without help from IT.

Remediating in safety

Recovering from a ransomware attack and bringing systems back online does not necessarily mean the attacker has left the environment. They might have tried to establish persistence to come back later. A common technique is to compromise existing accounts or create new accounts, often by accessing Active Directory or other directories containing user accounts. Duo MFA can bring the peace of mind that an attacker who is still on the network cannot easily pivot and move laterally using compromised credentials. It can also buy time and prevent an attacker from doing further damage while the attack is fully remediated, removing all traces of persistence.

Implementing a Zero Trust Security model

Built on the principle of "never trust, always verify," zero trust is a security model that can help organizations proactively implement best practices known to protect against cyberattacks, including ransomware.

Zero trust is so critical that the White House issued an executive order specifically mandating zero trust and MFA.

Duo provides MFA that's easy to use and implement. It also allows organizations to only grant access if a user and their device can be verified and trusted. This ability to control and manage access is one of the foundational pillars of zero trust, and Duo MFA is one of the first steps to implementing a zero trust framework.

Conclusion

Ransomware will be more prevalent and companies must be more vigilant. Social engineering and spear phishing are successful because they exploit the human element of an organization's security. Adopting and implementing a zero trust security philosophy that starts with strong MFA and a trusted access platform is important for staying ahead of ransomware attacks.

Update your defense beyond MFA With Duo

Organizations can defend against the impact of ransomware through social and targeted phishing attacks by implementing conditional access policies that leverage contextual factors, such as location and the device posture, in order to establish trust in users and their devices.

Duo's cloud-based security platform protects access to all applications, for any user and device, from anywhere. We've simplified secure access to address identity and device risks with six critical capabilities:

1. Verify users' identities with secure and flexible multi-factor authentication methods.
2. Deliver a consistent login experience with Duo Single Sign-On, providing centralized access to both on-premises and cloud applications.
3. Gain visibility into every device, and maintain a detailed inventory of all devices that access corporate applications.
4. Establish device trust through health and posture checks for managed or unmanaged devices before granting application access.
5. Enforce granular access policies to limit access to those users and devices that meet the organization's risk tolerance levels.
6. Monitor and detect risky login behavior using Duo Trust Monitor, or export logs to your SIEM, in order to remediate suspicious events such as new device enrollment for authentication or login from an unexpected location.

Why choose Duo?

Speed to security

Duo delivers the building blocks of zero trust in one solution that is fast and easy to deploy to users. Depending on their specific use case, some clients can be running in a matter of minutes.

Ease of use

Users can self-enroll as simply as downloading an app from the app store and signing in. Maintenance and policy controls are easy for admins to control and gain clear visibility.

Integrates with all applications

Our product is designed to be agnostic and work with legacy systems. No matter what IT and security vendors you use, with Duo you can still secure access to all work applications, for all users, from anywhere.

Lower Total Cost of Ownership (TCO)

Because Duo is easy to implement and doesn't require replacing systems, it requires far fewer resources in time and cost, quickly getting you up and running and begin the journey to a zero trust security model.

References

The Pandemic-hit World Witnessed a 150% Growth of Ransomware, https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, Mar 5, 2021

Exclusive: U.S. to give ransomware hacks similar priority as terrorism, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, Reuters, June 3, 2021

NIST Announces Tech Collaborators on NCCoE Zero Trust Project, https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/, Homeland Security Today, Sep 24, 2021

FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware, https://www.whitehouse.gov/briefingroom/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, The White House, Oct 13, 2021

Types of Encryption: Symmetric or Asymmetric? RSA or AES?, https://preyproject.com/blog/en/types-ofencryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, Jun 15, 2021

What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast, https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc, The Heritage Foundation, May 20, 2021

What We Can Learn From Ransomware Actor "Security Reports," https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, June, 24, 2021

The State of Ransomware 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx, Sophos, 2021

Data Mining Process: The Difference Between Data Mining and Data Harvesting, https://www.import.io/post/the-difference-between-data-mining-data-harvesting, Import.io, Apr 23, 2019

Ransomware: Enemy at The Gate, https://ussignal.com/blog/ransomware-enemy-at-the-gate, US Signal, Sep 3, 2021

2020 Data Breach Investigations Report, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, Verizon, 2020

Malware is down, but IoT and ransomware attacks are up, https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, June 23, 2020

One Ransomware Victim Every 10 Seconds in 2020, https://www.infosecurity-magazine.com/news/oneransomware-victim-every-10/, Infosecurity Magazine, Feb 25, 2021

Terrifying Statistics: 1 in 5 Americans Victim of Ransomware, https://sensorstechforum.com/1-5-americansvictim-ransomware/, Sensors Tech Forum, Aug 19, 2019

Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-and-risk-managem, Gartner, May 17, 2021

1 in 5 SMBs have fallen victim to a ransomware attack, https://www.helpnetsecurity.com/2019/10/17/smbsransomware-attack/, Help Net Security, Oct 17, 2019

Ransomware – how to stop this growing, major cause of downtime, https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime, Polyverse.com

The strange history of ransomware, https://theworld.org/stories/2017-05-17/strange-history-ransomware, PRI The World, May 17, 2017

Ransomware Timeline, https://www.tcdi.com/ransomware-timeline, tcdi.com, Dec 27, 2017

A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time, Digital Guardian, Dec 2, 2020

One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5, Business Insider, May 22, 2021

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare, https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare, Wired.com, Apr 23, 2018

Cyber-attack: US and UK blame North Korea for WannaCry, https://www.bbc.com/news/world-uscanada-42407488, BBC.com, Sep 19, 2017

Ransomware: Now a Billion Dollar a Year Crime and Growing, https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646, NBCNews.com, Jan 9, 2017

The Untold Story of NotPetya, the Most Devastating Cyber Attack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Wired.com, Aug 22, 2018

Ransomware in Healthcare Facilities: The Future is Now, https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty, Marshall University Digital Scholar, Fall 2017

New ransomware holds Windows files hostage, demands $50, https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html, NetworkWorld.com, Mar 26, 2009

Preventing Digital Extortion, https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, May 2017

The Irreversible Effects of Ransomware Attack, https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack, CrowdStrike, July 20, 2016

New Era of Remote Working Calls for Modern Security Mindset, Finds Thales Global Survey of IT Leaders, https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders, Business Wire, Sep 14, 2021

FBI sees spike in cyber crime reports during coronavirus pandemic, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic, The Hill, Apr 16, 2020

Symantec Security Summary – September 2021, https://symantec-enterprise-blogs.security.com/blogs/featurestories/symantec-security-summary-september-2021, Symantec Security, Sep 27, 2021

INTERPOL report shows alarming rate of cyberattacks during COVID-19, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, Interpol, Aug 4, 2020

Gartner Top Security and Risk Trends for 2021, https://www.gartner.com/smarterwithgartner/gartner-topsecurity-and-risk-trends-for-2021, Gartner, Apr 5, 2021

Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time, Gartner, July 14, 2020

Gartner Highlights Identity-First Security as a Top Security Trend for 2021, https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021, Attivo, Apr 27, 2021.

2021 SonicWall Cyber threat Report, https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf, SonicWall, 2021

Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme, https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme, ZDNet.com, Aug 23, 2020

VPN exploitation rose in 2020, organizations slow to patch critical flaws, https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/, Cybersecurity Dive, June 18, 2021

New research: How effective is basic account hygiene at preventing hijacking, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, Google Blog, May 17, 2019

Top cybersecurity statistics, trends, and facts, https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html, CSOonline.com, Oct 7, 2021

Protecting Companies From Cyberattacks, https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html, Inc.com, Sep 20, 2021

ThreatList: People Know Reusing Passwords Is Dumb, But Still Do It, https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, May 25, 2020

Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components, https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, May 12, 2020

Ransomware's Dangerous New Trick Is Double-Encrypting Your Data, https://www.wired.com/story/ransomware-double-encryption/, Wired.com, May 17, 2021

Combating Lateral Movement and the Rise of Ransomware, https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, June 24, 2021

Lateral Movement, https://attack.mitre.org/tactics/TA0008/, MITRE| ATT&CK, Oct 17, 2019

Industries Impacted by Ransomware, https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Defend Against and Respond to Ransomware Attacks, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, Gartner Research, Dec 26, 2019

Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, The White House. May 12, 2021