WHITE PAPER

Keysight Technologies 2021 Security Report

Introduction

Welcome to the fourth edition of this Security Report issued by Keysight Technologies, and formerly Ixia. This report combines lessons learned in 2020 with impactful predictions for 2021. Both the data and the predictions are based upon research conducted by Keysight's Application and Threat Intelligence (ATI) Research Center.

Monetary gain took center stage as a key cybercrime motivator. There was a huge uptick in the deployment of ransomware starting in June with 59% of attacks occurring in the 2nd half of 2020. While this trend was directed across all industries, healthcare was hit especially hard.

The purpose of this report is to help strengthen global cybersecurity. Effective cybersecurity needs to be a collaborative function by security experts. This report is one way of sharing what Keysight has learned over the past year with the international community of security practitioners. We hope it will help security teams think about their security architecture vulnerabilities and how they can better prepare for future attacks.

There were three trends that characterized cybercrime for most of 2020:

- Cybercrime did not take a holiday during the pandemic. Keysight research shows that there was a 62% increase in phishing attacks in 2020 over 2019. In fact, we saw a rapid increase as the pandemic took center stage in March and April.
- Monetary gain took center stage as a key cybercrime motivator. There was a huge uptick in the deployment of ransomware starting in June. While this trend was directed across all industries, healthcare was hit especially hard. The second half of 2020 was particularly brutal with 59% of the attacks occurring during that timeframe.
- Supply chain attacks hit the headlines with the SolarWinds attack. The supply chain continues to be a weakness since the infamous Target point of sale breach in 2013 brought this type of risk to the forefront. The SolarWinds attack reinforces the need for security architects to embrace a holistic and comprehensive approach.

In this report, we'll look into three core attack vectors used in 2020 along with what you need to know to thwart those attacks. The last section discusses the main relevant threats we see for 2021.

KEYSIGHT TECHNOLOGIES

Key Findings from 2020

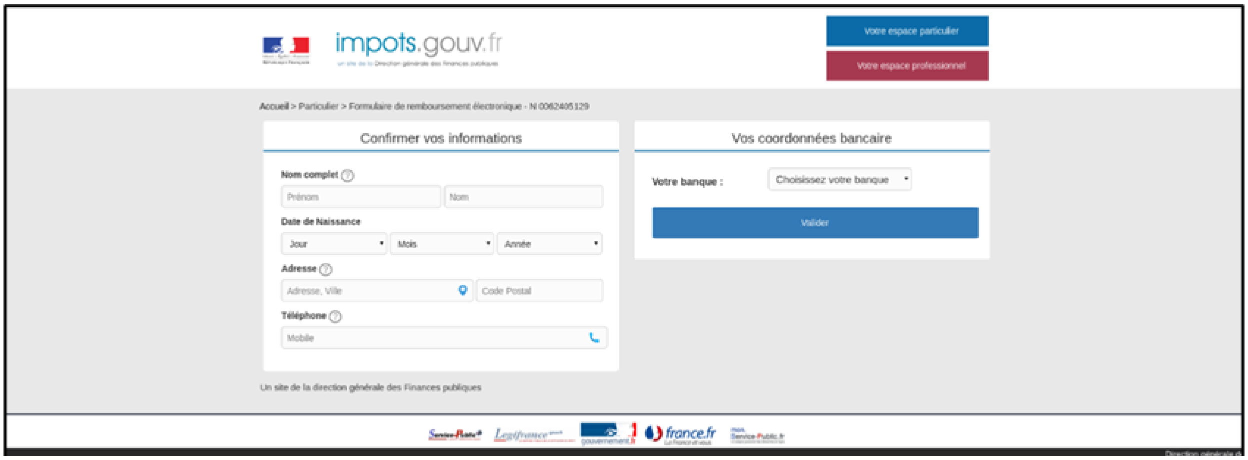
Throughout history, cybercriminals have shown that they are opportunistic in nature. If they know of a weakness, technological or human, they will try to take advantage of it. We saw plenty of evidence supporting this in 2020 and we'll examine three key attack vectors that took place in the following sections:

1. Phishing in a pandemic
2. Ransomware attacks on healthcare providers during 2020
3. The most effective supply chain attack to date

Phishing In A Pandemic

Keysight research shows that there was a 62% increase in phishing attacks in 2020 over 2019. People trying to get financial or healthcare assistance were ripe targets for COVID-19 phishing campaigns. Governments from around the world have been helping their citizens through reimbursements and financial support to small businesses and unemployed people. However, this move meant malicious actors updated their methods of attack, resorting to phishing to take advantage of people trying to benefit from such government-sponsored benefits.

Figure 1 shows an attempt to capture personal information from French citizens using a fake government website page. Note – the link below has been altered to prevent anyone from clicking it.



impots.gouv.fr

Votre espace particulier

Votre espace professionnel

Accueil > Particulier > Formulaire de remboursement électronique - N 0062405129

Confirmer vos informations

Nom complet: Prénom, Nom

Date de Naissance: Jour, Mois, Année

Adresse: Adresse, Ville, Code Postal

Téléphone: Mobile

Vos coordonnées bancaire

Votre banque : Choisissez votre banque

Valider

Un site de la direction générale des Finances publiques

Figure 1. Fake French government webpage found at hxxps:[//]goovcovid19[.]com/impotgov/remboursement/bc6dc/

Keysight has been tracking these phishing attempts. In Figure 2 we can see that 61% of the COVID-19 related phishing pages were created in the first three months of the transition to work from home — March, April, and May of 2020, with far fewer web pages created in the following months.

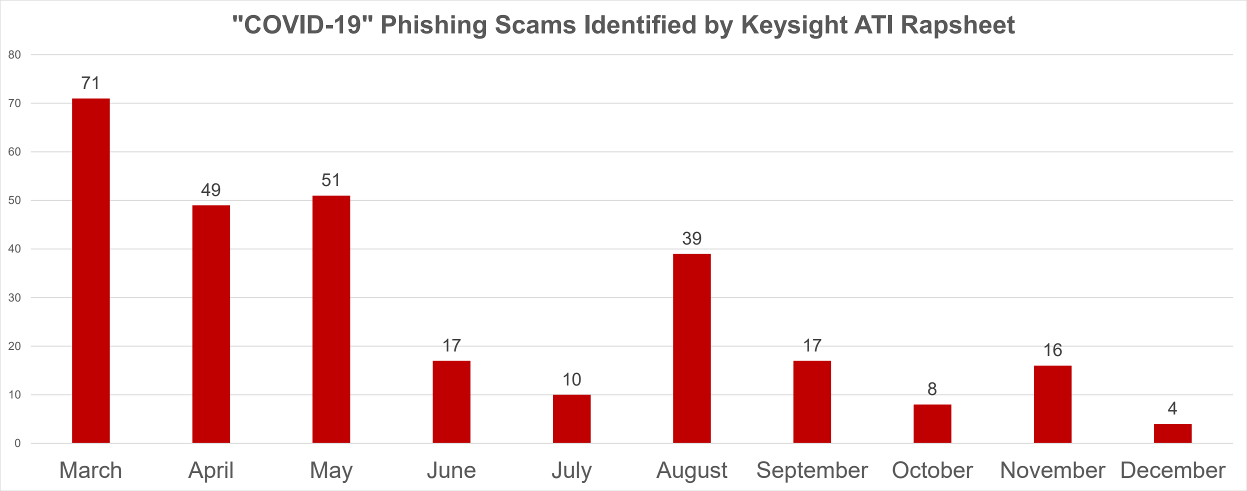


Figure 2. COVID-19 specific phishing attacks by month in 2020 (Keysight Technologies ATI research)

Looking at the targeted websites in Figure 3, we can clearly see that malicious actors preferred to target victims using pages mimicking those of financial institutions — Chase, ATB, Paypal, Simplii, and Americanas. While social media accounts were also targeted, it's clear that monetary gain was the main driver for phishing attempts.

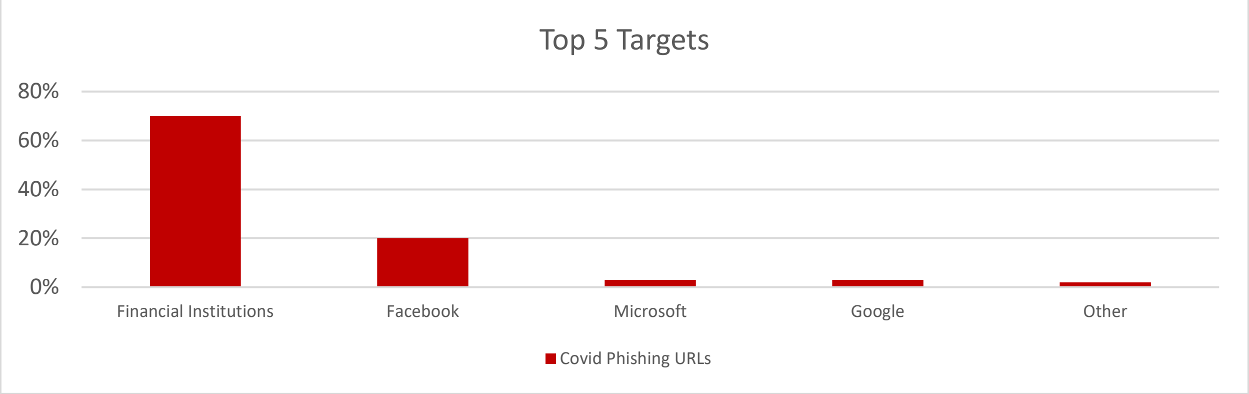
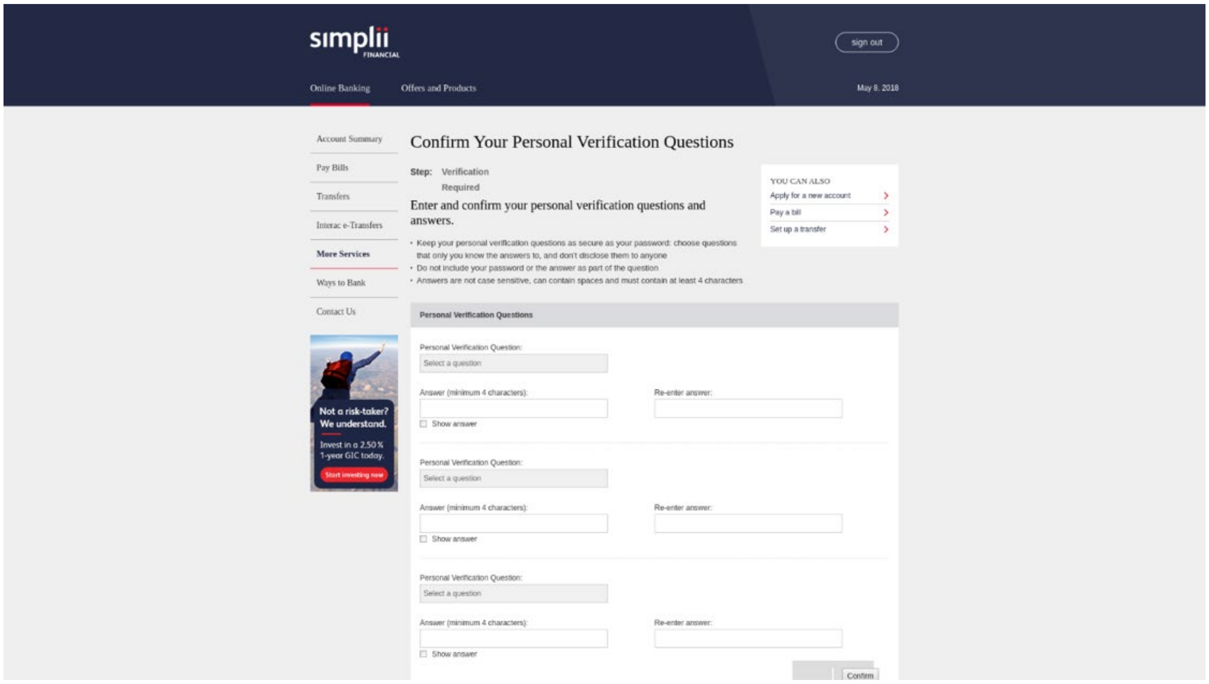


Figure 3. Top five groupings of mimicked phishing attacks (Keysight Technologies ATI research)



Confirm Your Personal Verification Questions

Step: Verification Required

Enter and confirm your personal verification questions and answers.

- Keep your personal verification questions as secure as your password: choose questions that only you know the answers to, and don't disclose them to anyone
- Do not include your password or the answer as part of the question
- Answers are not case sensitive, can contain spaces and must contain at least 4 characters

Personal Verification Questions

Personal Verification Question: Select a question

Answer (minimum 4 characters): Re-enter answer:

□ Show answer

Personal Verification Question: Select a question

Answer (minimum 4 characters): Re-enter answer:

□ Show answer

Personal Verification Question: Select a question

Answer (minimum 4 characters): Re-enter answer:

□ Show answer

Figure 4. Sample phishing page found at hxxps:[//]covid19lssuedbill[.]com[/]directing[/]Simplii/details.htm

Strategic Insight #1: Phishing and additional social engineering attacks will continue to take advantage of pandemic-related headlines, as we've seen with bogus testing and vaccination scams. And now that vaccines are availabile, expect to find cyber criminals moving on to target vaccination registration. This means that people looking to get vaccinated need to be educated to recognize a vaccination scam and must be awared that bad actors target personally identifiable information (PII) in a healthcare setting. Avoid clicking on links in emails and text messages; go directly to your trusted healthcare site and find the registration link. And next year, we expect to see the same criminal activity around booster shots.

Ransomware Attacks on Healthcare Providers During 2020

Ransomware continued to be one of the leading threat vectors seen in 2020, again with the goal of direct financial benefit for the hackers. Industries like healthcare were prime targets. The United States Cybersecurity and Infrastructure Security Agency (CISA) posted a warning on October 28, 2020 to this effect, "There is an imminent and increased cybercrime threat to U.S. hospitals and healthcare providers."[1] The warning specifically included Trickbot and Ryuk ransomware, and (though CISA's purview is the United States) how ransomware impacted healthcare providers across the globe.

This especially cruel act of encrypting files and systems en masse and then, holding data hostage for ransom~~,~~ does not seem to be going away. While the cybercriminals are not always picky with who they can get with ransomware,-the strain on healthcare providers last year made them especially attractive targets. Another trend we saw was the combination of decrypting data in exchange for payment with the

[1] "U.S. Hospitals Targeted In Rising Wave Of Ransomware Attacks, Federal Agencies Say," NPR. October 29, 2020. https://www.npr.org/2020/10/29/928979988/u-s-hospitals-targeted-in-rising-wave-of-ransomware-attacks-federal-agencies-say

added threat of releasing said data publicly if the attackers weren't paid. Of course, even if the ransoms were paid, there's no guarantee that stolen data wouldn't be leaked at some point in the future.

Ransomware and credential theft also spread among many individuals through the use of phishing with news related to COVID-19. Some ransomware authors claimed they wouldn't target healthcare facilities during the pandemic[2] in March, although the honesty of such individuals was always in question[3]. These new ransomware campaigns were evolutions of existing malware strains focused on new targets, and not novel new strains of malware.

While ransomware attacks in the first five months of 2020 were somewhat low, Keysight research in Figure 5 shows that April saw a spike of over 13,000 attacks and June saw a huge spike over 30,000 attacks. The large numbers of attacks continued throughout the rest of 2020 with the 2nd half of the year encompassing 59% of the 107,781 attacks.

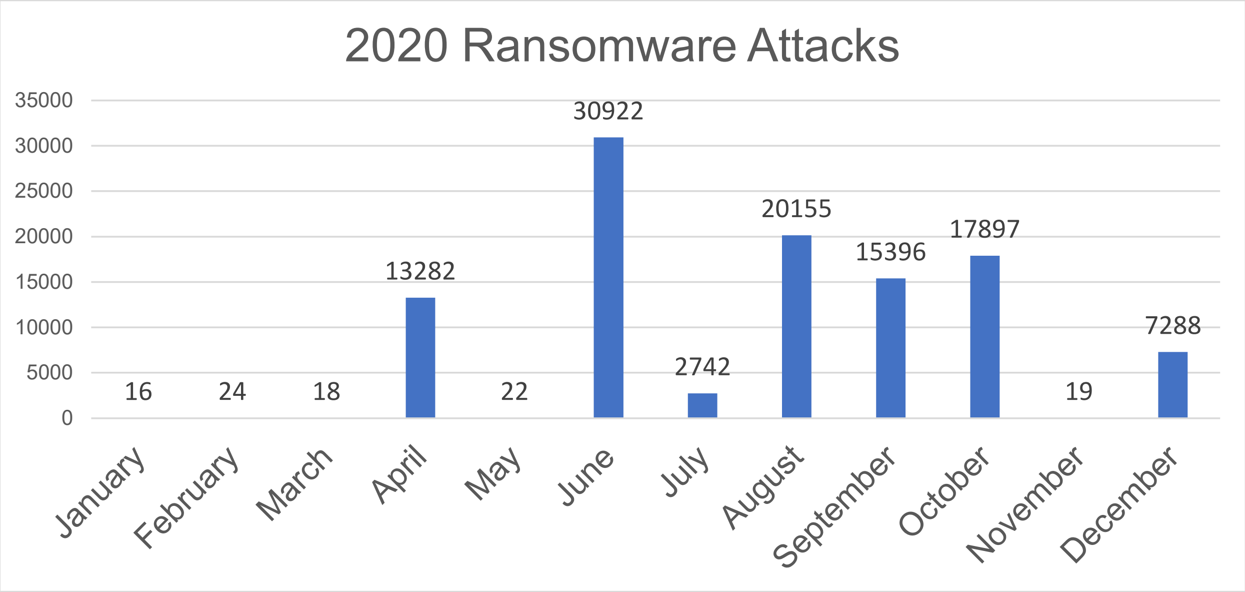


Figure 5. Ransomware attacks launched in 2020 (Keysight Technologies ATI research)

Ransomware Lowlights

Snake

Snake is a ransomware variant that first appeared in January of 2020.[4] It gets its name from leaving a telltale string at the end of an encrypted file with words SNAKE in reverse (EKANS). Snake's first recorded attack on a healthcare facility occurred in early May at Fresenius Group, the largest private hospital operator in Europe.[5] Snake is written in Golang, a language first developed at Google in 2007 to

[2] "Ransomware Gangs to Stop Attacking Health Orgs During Pandemic," Lawrence Abrams, Bleeping Computer. March 18, 2020. https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

[3] "Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack," Bill Goodwin, Computer Weekly. March 22, 2020. https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

[4] "SNAKE Ransomware Is the Next Threat Targeting Business Networks," Lawrence Abrams, Bleeping Computer. January 8, 2020. https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/

[5] "Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware," Brian Krebs, Krebs On Security. May 6, 2020. https://krebsonsecurity.com/tag/snake-ransomware/

take advantage of multicore architectures and enable more productive programmers. Golang is an interesting choice for malware authors to choose, since it can imply an intent to move the malware into a multiplatform environment later with relative ease. Snake's primary targets have been industrial control systems (ICS), including reported campaigns at Honda and Enel Group.[6] Its initial vector of infection has been targeting systems with Remote Desktop Protocol (RDP) enabled and weak passwords in use. Once infected, it attempts to kill a variety of remote systems management processes, including Honeywell's HMIWeb which is used in operation of ICS systems.

Trickbot and Ryuk

Trickbot is another malware variant that has been around for a long time but has recently been refocused on targeting healthcare during the pandemic. TrickBot was first discovered by Fidelis Security in 2016[7], but national attention didn't really appear until the fall of 2020, when the CISA released a report detailing its widespread usage in healthcare and public health sector facilities.[8] TrickBot has a full suite of tools to conduct illegal cyber activities, including credential theft, crypto mining and deploying ransomware.

Keysight performed and documented a detailed analysis of Trickbot and Ryuk.[9] Through this analysis, we've seen TrickBot deployed as a Windows Word document that leverages both macros and XXE techniques to gain footholds within targets. In the last year, Trickbot was seen deploying the Ryuk family of ransomware across multiple health care facilities. Ryuk leverages off-the-shelf command and control infrastructure tools such as Empire or Cobalt Strike. Both TrickBot and Ryuk leverage older vulnerabilities to spread; indicating that health care facilities might not have the most up to date operating systems available or suffer from lagging patch management solutions. Ryuk malware infections caused some hospitals to redirect ambulances and relocate patients in need of surgery.[10]

Maze

Maze is another common ransomware variant that has caused disruptions in the health-care industry. Just after a week of notifying a reporter for the Bleeping Computer news agency that they would not target health care sites, the bad actor group infected Hammersmith Medicines Research (a COVID-19 testing facility in the UK) in mid-March.[11] According to the report, the Maze malware stole copies of testing data and published it online. These documents included: date of birth, passports, driving licenses, visa documents, health questionnaires, and consent forms. This attack highlights the fact that data needs to be encrypted when at rest, as well as in motion. Maze does not appear to target healthcare facilities specifically, as the biggest successful Maze breach last year was with the IT

[6] "Snake ransomware poses unique danger to industrial systems," Alexander Kulafi, TechTarget Search Security. July 1, 2020. https://searchsecurity.techtarget.com/news/252485531/Snake-ransomware-poses-unique-danger-to-industrial-systems

[7] "TrickBot: We Missed you, Dyre," Fidelis Cybersecurity. October 15, 2016. https://fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/

[8] "Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector," United States Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[9] "TrickBot: A Closer Look," Keysight blog. https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2020/12/21/trickbot_a_closerl-TpQ0.html

[10] "UHS restores IT service to hospitals, corporate data centers following massive ransomware attack," Heather Landi, Fierce Healthcare. October 6, 2020. https://www.fiercehealthcare.com/tech/uhs-restores-it-service-to-hospitals-corporate-data-centers-following-massive-ransomware

[11] "HMR targeted by cyber criminals," Hammersmith Medicines Research. April 29, 2020. https://www.hmrlondon.com/hmr-targeted-by-cyber-criminals

services firm Cognizant.[12] Maze acts like a worm, not only infecting the machine on which it is present, but leveraging that machine to infect adjacent machines it discovers on the network by utilizing common set of remote vulnerabilities.

Strategic Insight #2: Ransomware is highly popular because it makes a lot of money for bad actors. While it's not going away, business models continue to mutate along with malware variants. On the detection side, it's critical to keep your threat detection systems up to date with the latest signatures and behavioral patterns, as ransomware builders are getting better at obfuscation and avoiding detection. You should also be aware that exploitation practices are changing, as enterprises have gotten better at making secure backups to avoid needing to pay ransom. Hackers are increasingly turning to the threatening the release of sensitive data which can trigger penalties, intellectual property loss, and sever reputational impact.

The Most Effective Supply Chain Attack to Date

On December 8th, 2020 FireEye acknowledged they suffered a breach and that their *Red Team* tools had been stolen by an unidentified threat actor.[13] The investigation continued and on December 11th the world was taken by storm — FireEye was just a collateral victim. They had been hacked through a weaponized SolarWinds update.

SolarWinds has around 300,000 customers of which 18,000 of them were a potential victim of this supply chain attack, which leveraged their Orion software. Potential victims include: Microsoft, VMware, various municipalities and utilities, and government agencies such as the Departments of Defense, Commerce, Energy, Justice, and Homeland Security. The investigation continued on the SolarWinds side and it was uncovered that the first suspicious activity happened in September 2019. Back then, the attackers tested their capability to insert malicious code into the SolarWinds build process. The test code injection ended two months later in November 2019. In February 2020, they inserted the actual malware. The code was built and signed by SolarWinds and the update was released for customers to download and execute.

In June 2020, the attackers then removed the malware from the build virtual machines. The attackers remained undetected for more than one year, from September 2019 to December 2020. During this timeline, two customer incidents were reported, but no resolution was provided at that time and the malware remained undetected. Vulnerabilities in the platform were investigated or remediated, but the malware was still not detected.

The malicious code implanted in the Orion downloads was exceptionally stealthy. After a dormant period of up to two weeks, the malware would phone home to domestic command and control sites. This malicious traffic wasn't immediately obvious, blending in with legitimate SolarWinds activity and passing as the Orion Improvement Program (OIP). The jobs executed include file transfer, file execution, system profiling, rebooting the system, and disabling services. To maintain a low footprint, the attackers used legitimate credentials to achieve remote access. This is how FireEye discovered the supply chain attack

[12] "Maze Ransomware Attack on Cognizant May Impact Customers," Alicia Hope, CPO Magazine. May 1, 2020. https://www.cpomagazine.com/cyber-security/maze-ransomware-attack-on-cognizant-may-impact-customers/

[13] "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," Kevin Mandia, FireEye blog. https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

— they noticed a suspicious authentication to their VPN solution. The attackers were able to enroll a new device into the multi-factor authentication (MFA) solution, which triggered an alert.

The steps of this attack are illustrated in Figure 6 the image below:

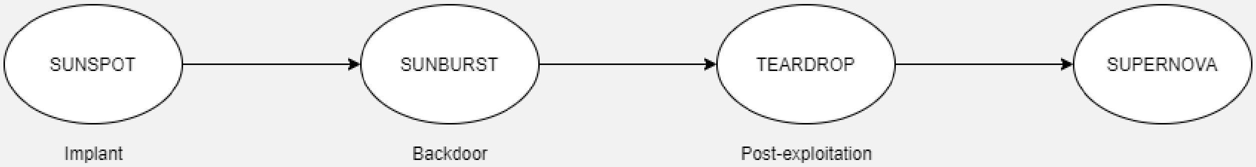


Figure 6. Sequence of malware attacks within the SolarWinds attack.

The never-before-seen combination of techniques is what makes this campaign unique and so hard to detect. There are four basic stages to the attack:

1. SUNSPOT – Malware which was responsible for monitoring the SolarWinds build system and injecting the SUNBURST malware in the generated builds.
2. SUNBURST – Malware that was embedded code within the SolarWinds Orion platform that would sit and listen for command and control (C2) instructions. This attack would obtain C2 IP addresses located in victim's country to help mask itself.
3. TEARDROP – Malware that was delivered through the C2 instructions sent from SUNBURST. This malware makes use of steganography to conceal messages and the installation of other programs. This included temporary file replacement and temporary task modification.
4. SUPERNOVA – This consisted of a web shell specially designed to work with SolarWinds Orion products.

It's also important to note that our knowledge of the attack is limited to what we've discovered thus far; because of the elevated permissions granted to SolarWinds Orion installations, subsequent malware is able to run with elevated permissions. The design of attack essentially resembles a Matryoshka doll, with executable stages nested within containerized units. So even if you identify one infection, you aren't sure if you got it all. It's possible that malware pushed into networks may still be lying dormant or undetected even if the corrupted SolarWinds software has been removed. Continued monitoring and anomaly detection are recommended for anyone who installed the affected Orion software as a precautionary measure.

So What Have We Learned From SolarWinds

Additional Strategic Insights:

3. Your supply chain is more than just your components. There is a tendency to think of your supply chain as outside entities that either supply you with software and hardware components or the supplies you use when building your product. However, as we've learned, it goes beyond that. Your supply chain is anything critical to the operation of your business. This includes everything

from your utilities, to your email, to your cloud provider, and perhaps even your coffee supplier. If you can't do business without it, or if corruption or interruption to something you use causes you to lose time, money, or revenue, then it's part of your supply chain and it's important. For instance, a recent cyberattack against Molson Coors halted their production facilities for a period of time.

4. Zero-trust is more than just a buzzword. And it doesn't just mean limiting what your users can see when they connect to your network. A successful zero-trust implementation means that systems and users can only access the internal or external resources that they absolutely need. Zero-trust couldn't stop an Orion server from downloading the corrupted update, but it could have prevented it from connecting out to the C2 server it needed to download additional malware, thus protecting an enterprise from any negative impact.
5. Lastly, assume you're breached, and behave accordingly. This is the driving motivation behind zero-trust — assume that an entity might be breached so that you limit the scope of what resources it can access and modify. It also underscores the importance of visibility. If you can't spot anomalies hiding in your network (whether on-premises, in the cloud, or a remote user), then you're allowing breaches to remain undetected indefinitely. With the SolarWinds breach, complete DNS visibility and logging of connections from the Orion server would have provided the telltale signs of infection, enabling both detection and forensic analysis.

Looking Forward, 2021 and Beyond

For most of us, 2021 still feels like the extended dance mix of 2020. The SolarWinds breach just added onto the pile of recent IT challenges including the pandemic-related rush to work remotely and phishing attacks. However, stepping back and taking a look at the big picture, the narrative has been largely unchanged for years. We are still in a world where cybersecurity is mostly immature and looked at from a 'how do I prevent it' or 'how do I avoid it' perspective. We at Keysight believe that the world needs to look at it from a 'how can I detect and be resilient' perspective. The active breach inside your network is not a matter of if, but of when. Will you be ready?

We believe 2021 is the year that the network security for 100% of enterprises will reach the *compromised* status level, whether the organizations know it or not. The impacts of work from home, the move to support remote workers, and lack of preparedness have offered the bored cybercriminal with a plentiful supply of targets. Additionally, cybercriminals have continued to enhance their capabilities. They had a lot of time on their hands in 2020 to work on and improve their tools of the trade. This year will be filled with this realization as we uncover the artifacts of malicious activity in our networks. The faster we get to the point where we can find them, the sooner we'll be able to work on remediating the situation.

Visibility for Detection and Measurement

The quote, "You cannot manage what you cannot measure" by Peter Drucker, is one of the most relevant, yet underestimated, quotations which can apply to cybersecurity. The ability to measure an organization's cybersecurity preparedness, and security control efficacy, is essential to making qualified decisions and applying a security-in-depth model.

Why is proactive security measurement so important? One reason is that most breaches aren't due to poor technology. Most of the firewalls, endpoint detection and response (EDR) products, and network detection and response (NDR) solutions on the market are actually quite good at detecting or blocking attacks — if configured perfectly. But the complexity of managing dozens of security products, tracking daily changes in the threat landscape, and effectively triaging the millions of SIEM alerts which deluge SOC teams makes it easy to open up the one gap that attackers need to get in. Repeatable, comprehensive measurement of security posture is a critical step in maintaining effective security and maximizing value from security investment. The prevalence of breaches caused by simple misconfiguration is amply supported by industry research; Gartner notes that “through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.”[14]

In their 2020 Data Breach Investigation Report, Verizon reported a similar trend. Security breaches due to misconfiguration errors rose from 8th place in 2015 to 4th place in 2020, gaining a full 4.9% over the year before.[15] Phishing, of course, was the number one root of breaches according to the Verizon study.

There’s No Silver Bullet

This seems like an obvious statement. An organization’s cybersecurity solution is a mix of many different products and there’s no single point solution, the mythical *silver bullet*, that solves all cybersecurity problems. There is a complex set of security controls and policies that is only as strong as its weakest link. It’s therefore critical to be able to identify the weakest link and to remove and replace it, or to enhance it so it can perform as required. This starts with inline security solutions (like web application firewalls, decryption, and intrusion prevention solutions), but also includes packet analysis solutions (like data loss prevention and indicator of compromise investigative solutions).

Proactive and Continuous Assessments

Staying on top of all the moving parts of a complex security deployment isn’t trivial. Human-based testing regimes, such as Penetration Testing and Red Teaming exercises can certainly help identify specific weaknesses and train SOC teams. However, they tend to be expensive, non-repeatable, and not comprehensive. These two security practices proceed until the first exploitable vulnerability is found, then move deeper into the exploit without checking all other security controls.

Combining periodic human-based testing with more comprehensive automated software tools that perform exhaustive and repeatable assessments of tools, teams, and processes can yield a much better return on investment and deliver much shorter intervals between the opening and remediation of security vulnerabilities.

Conclusion

This report concludes with the following key takeaways:

- Act like your network has already been compromised
- Create a plan to quantify risk and impact
- Assess and validate your current operations

If your network has been compromised, what should you be doing right now? An obvious activity would be to look for any indicators of compromise. However, do you have everything you need to actually

[14] Gartner, Technology Insight for Network Security Policy Management, Rajpreet Kaur, et al., Refreshed 20 May 2020, Published 21 February 2019.

[15] “Data Breach Investigations Report”, Verizon. Published May 19, 2020.

perform that investigation? Do you have the data collection infrastructure — the taps and packet brokers that you need? Do you have the security tools you need in place — DLP, IDS, and DPI solutions?

For instance, the focus is often on the wrong place. Security engineers often pay too close attention to the malware or the fix. You also need to look for lateral movement. Know your network by understanding the expected and improve on identifying the anomalies.

Next, can you quantify risk and impact? If not, how will you be able to prioritize issues, i.e. how will you be able to sort the wheat from the chaff? Risk is everywhere and in every decision. For instance, the SolarWinds breach stood out for impacting those who followed best practices and kept their software up to date — all of which are considered best practices. While these practices reduced risk, they also created a new risk, highlighting that there's no one practice which will keep the enterprise safe. You need to map out your security architecture decisions and the risk associated with each layer — from physical hardware/software to policies to preproduction and postproduction validation.

Lastly, can you assess or validate your operations? While Penetration Testing is an important part of your security architecture validation process, you need to be able to test the production network whenever necessary. This includes routine checks of architecture performance as well as validation of the correctness and efficacy of any configuration changes to the architecture. Do you have vulnerable equipment or segments — you need to know?

About the ATI Research Center

The Keysight ATI Research Center is an elite group of dedicated network security professionals. Its purpose is to stay current with ever-evolving changes that could impact the security of IT networks. The team then distills that knowledge into research which can be incorporated within Keysight solutions to keep up with continually evolving threats.

The ATI team is distributed across the world in locations like Singapore, California, Texas, Massachusetts, France, Romania, and India so that there is always a part of the team that is looking for new threats to analyze.

The ATI team also contributes to the larger security community. It is not just about us. Our team also shares what we learn with vendors that have been hacked, private agencies (e.g. www.mitre.org), government agencies (e.g. NIST and DARPA), and global security conferences like Black Hat and RSA. Keysight also promotes a summer security school in Bucharest, Romania to help train new security engineers.

The key goal for the ATI team is to assess and validate products that are meant to secure the enterprise. We do this by serving as a front line of defense to keep products from other vendors honest. Security alerts and incidents happen all over the globe and the team needs to be up around the clock. Dozens of engineers combine to form a single team that can create the intelligence and add to all product lines. In many cases, this lets the team go from discovery to product output within a twenty-four-hour period.

The exact input comes from many sources including:

- International exploit databases
- The “Dark Web”
- Scan of security news alerts and crowdsourcing
- Twitter handles of other security researchers
- Partner feeds
- Honeypots actively looking for attacks in the wild
- And independent research (testing and reverse engineering) by the ATI team

The team constantly polls multiple sources to get insights into vulnerabilities. This data is then normalized, processed, analyzed, and organized to get a clear direction on the threats, and how to prioritize them. Threats are investigated by team members and either validated or dismissed. The team validates everything to make sure that the content deployed in our products is 100% sure and correct. This gives the team the utmost confidence in our data and predictions.

The ATI team was established in 2005 as part of the BreakingPoint company. BreakingPoint was acquired by Ixia in 2012 and then Ixia was acquired by Keysight Technologies in 2017. The BreakingPoint solution is a security attack and traffic generator used by network equipment manufacturers, service providers, governments, and enterprises, to validate network and security resiliency while under load and attacks. The threat intelligence information incorporated into Keysight enterprise visibility solutions and now into Keysight automotive and Internet of things (IoT) solutions.

The threat intelligence feed from the ATI team is unique. They set an incredibly high bar for threat intelligence so that customers can completely trust it. While others in the industry create automated intelligence platforms or open source feeds, those solutions are not validated as thoroughly for accuracy as the Keysight solution. As an example, other intelligence information feeds can end up being focused on a specialized attack on a particular product (e.g. Cisco or Microsoft) instead of being related to the global picture of what is happening on the Internet.

For the Keysight ATI team, the intelligence is assembled into a “rap sheet”. Rap sheets are a proprietary database of known bad information or offenders. These lists are constantly updated. For instance, the teams recheck blacklisted sites every day to ensure that any false positives are removed. Automated fap sheets are continually updated every five minutes. This information can then be delivered to different product offerings.

Keysight is committed to making it as hard as possible for hackers to succeed.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus