SEQURETEK

SIMPLIFY SECURITY

2021

A Year In Review

TLP: GREEN

2021 RECAP

As in previous years, there has been an ever-increasing flood of stories of malware campaigns and data breaches in 2021. Security issues, such as the vulnerabilities in SolarWinds and Log4J, have brought home the fact that it is not enough to focus on your own environment but also on the all the pieces that make up your infrastructure. Security professionals now need to also investigate the components that come from diverse sources along with an expanded attack surface.

At Sequretek, we monitor 120+ different devices belonging to our customers spread across all sectors (financial, manufacturing, retail, e-commerce and pharmaceutical). Driven by our AI/ML based XDR, with an integrated global threat and malware intelligence feed, our Security Operation Centre has an expanded view of the threats as they arise.

In this year-ending release, we briefly cover the security issues and patterns that we observed.

ProxyShell

ProxyShell is the result of three vulnerabilities (CVE-2021-34473,CVE-2021-34523,CVE-2021-31207). ProxyShell is targeting on-premise installations of Microsoft Exchange Servers. When chained, these vulnerabilities allow the attacker to bypass ACL controls, send a request to a PowerShell back-end, and elevate privileges, effectively authenticating the attacker and allowing for remote code execution via port 443.

ProxyLogon

ProxyLogon is pre-authentication vulnerability (CVE-2021-26855) in Exchange Servers that allows a remote actor to bypass authentication and receive admin server privileges. Combined with a post-authentication vulnerability (CVE-2021-27065) that allows arbitrary file writes to the system, an actor can achieve remote command execution of arbitrary commands through internet-exposed Exchange Servers. Initial access is achieved through uploading a web shell called “China chopper.”

Most talked vulnerabilities of 2021

We were still grappling with the fallout of SolarWinds when ProxyShell and ProxyLogon hit the organisations. Barely had the dust settled from these then we were confronted with PrintNightmare.

As the year now fades away, organisations and security professionals are waking up to Log4Shell – and this looks to be a reoccurring theme as we head into 2022.

PrintNightmare

A remote code execution vulnerability, CVE-2021-34527, exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Log4Shell

A vulnerability in a widely used Java logging library, Log4j, was publicly disclosed along with proof of concept (PoC) code that exploits the vulnerability. An attacker can run arbitrary code by forcing the application or server to log a specific string by modifying the logging configuration file. This string can force the vulnerable system to download and run a malicious script from the attacker controlled system, which would allow them to effectively take over the vulnerable application or server.

Major Data Breaches of 2021

Facebook user data breach

More than 500 million Facebook users' details like names and genders, dates of birth, location, relationship status and employer were published online on an underground website. The data breach occurred by exploiting a vulnerability reportedly fixed in August of 2019. Facebook said the data was old, from a previously reported leak in 2019.

T-Mobile

T-Mobile data hack exposed the sensitive information of more than 50 million current, former, and prospective customers. About 7.8 million customer's names, dates of birth, social security numbers, driver's licenses, phone numbers had been stolen in the breach. Another 40 million former or prospective customers had their names, dates of birth, social security numbers and driver's licenses were subsequently leaked. As we write this, there are reports of another, smaller data breach. Affected customers could have had both their private CPNI viewed as well as their SIM card swapped.

Microsoft Exchange Bug Exposes 100,000 Windows Domain Credentials

Bugs in the implementation of Microsoft Exchange's Autodiscover feature have leaked approximately 100,000 login names and passwords for Windows domains worldwide. Unique credentials leaked from various applications such as Microsoft Outlook, mobile email clients and other applications interfacing with Microsoft's Exchange server.

Rise of the Double Extortion Ransomware

Double extortion, also known as pay-now-or-get-breached methods, is a growing ransomware strategy that threatens users. Ransomware attackers first steal information stored on a victim's machine before encrypting it. The attackers then make an additional demand to pay up to prevent the attackers from publishing their data online.

Sequretek reported on an increasing trend of double extortion attacks. Some of the prominent double ransomware families that we spotted in 2021 are tabulated below.

Ako/Medusa Locker	Egregor	Moun tLocker/Astro Locker	RanzyLocker/ ThunderX
Alumni Locker	Ekans	Nefilim	REvil/Sodinokibi
Avaddon	Everest	Nemty	Ryuk
Babuk Locker	Exx/Defray777	NetWalker	Snatch
Clop	Hades	ProLock	Sodinokibi
Conti	HelloKitty	RagnarLocker	SunCrypt
CryLock	LockBit	Ragnarok	Thanos
DarkSide	Maze	RansomExx	Xinof
DoppelPaymer	Mespinoza/Pysa		

Supply Chain Attacks

Supply chain attacks have been a concern for cybersecurity experts for many years because the chain reaction triggered by one attack on a single supplier can compromise a network of providers.

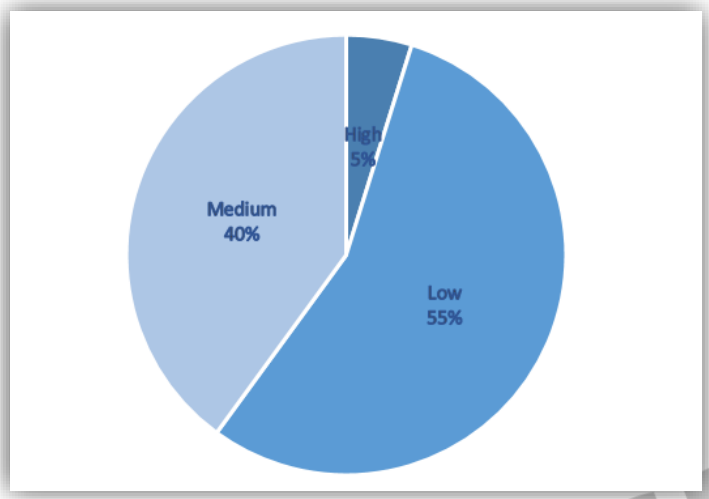
On December 13, 2020, FireEye announced the discovery of a highly sophisticated cyber intrusion that leveraged a commercial software application made by SolarWinds. It was determined that the advanced persistent threat (APT) actors had infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded the compromised version of installation packages from SolarWinds, attackers were able to access the systems running the SolarWinds product(s). This attack was exceptionally complex and continued to evolve well into 2021. The attackers randomised parts of their actions making traditional identification steps such as scanning for known indicators of compromise (IOC) of limited value.

On July 2, 2021 IT firm Kaseya reported having suffered a supply chain attack. REvil ransomware attackers leveraged a zero-day vulnerability, CVE-2021-30116, in Kaseya remotely accessed internet facing Virtual System Administration (VSA) Servers against multiple managed service providers (MSPs) and on-premise customers. The attackers compromised and manipulated the patch distribution process and sent a fake update to deploy ransomware. The attackers combined supply chain attack with ransomware to infect large number of organisations. REVil (Sodinokibi) attackers have compromised more than million systems and demanding 70,000,000$ Bitcoin for recovery.

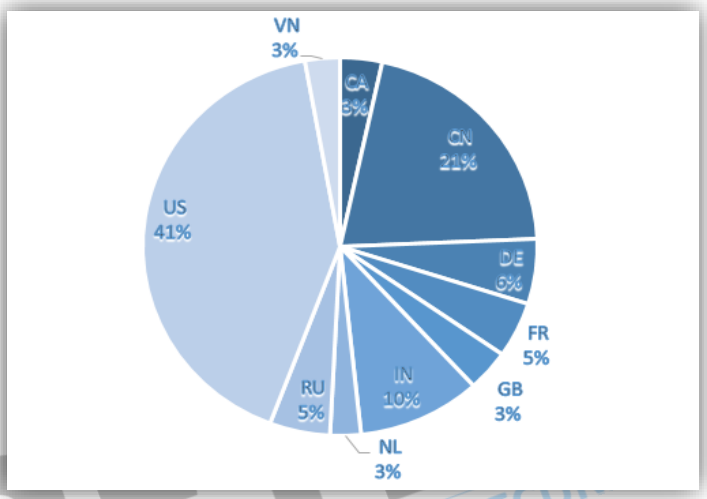
These are but a few samples of supply chain attacks that emerged in 2021. Sequretek believes that will become a dominant feature of the security landscape into the new year. The issues of discovering the vulnerable components, determining the attack surface, and rolling out updates, patches or configuration changes will contribute to increased headaches for security professionals.

Security Events and Incidents as Observed by our SOC

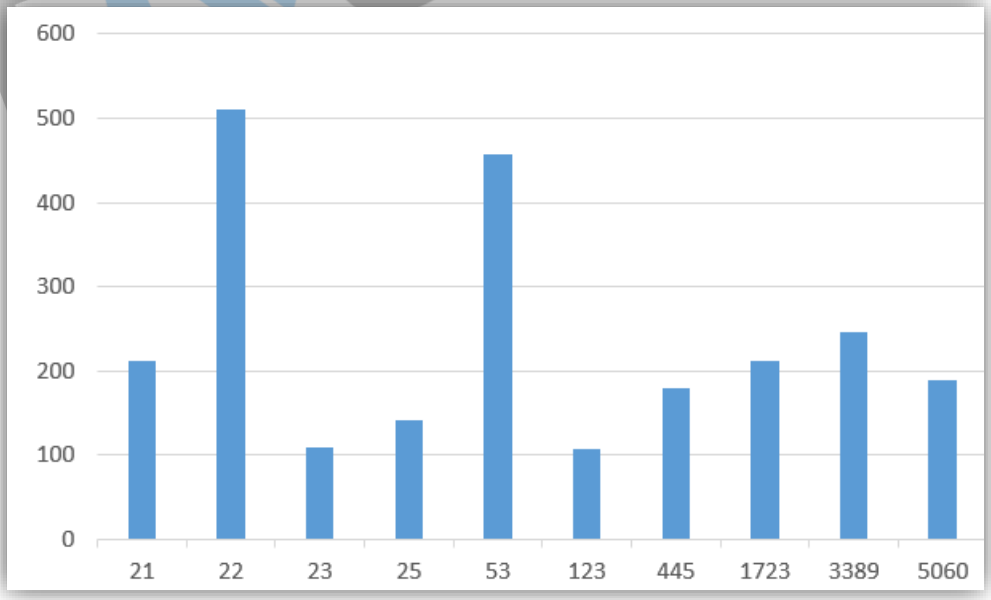
Risk Density



Top 10 Attack Origins



Critical Ports Commonly Scanned for Vulnerable Services



Exploitation Attempts Mapped to Vulnerabilities

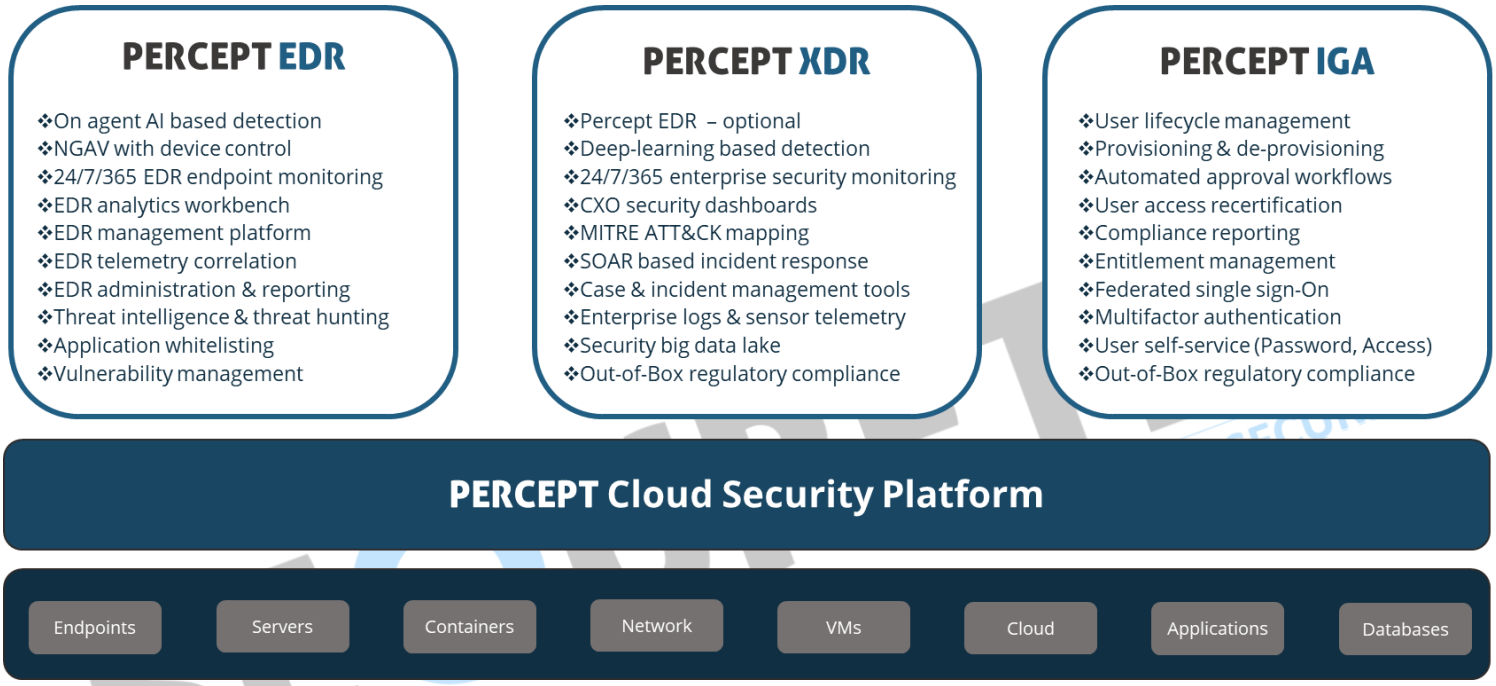
CVE-2003-1599	WordPress Remote PHP File Include Vulnerability
CVE-2007-1860	Apache mod_jk Directory traversal
CVE-2008-2938	Directory traversal vulnerability in Apache Tomcat 4.1.
CVE-2009-4458	Multiple cross-site scripting (XSS) vulnerabilities in FreePBX
CVE-2011-0013	Cross-site scripting (XSS) vulnerabilities in the HTML Manager Interface in Apache Tomcat
CVE-2011-1892	SharePoint Remote File Disclosure Vulnerability
CVE-2011-3600	XML-RPC SAX parser information exposure
CVE-2012-1823	PHP CGI Argument Injection
CVE-2015-0015	Network policy server RADIUS implementation denial of service vulnerability
CVE-2015-1635	Microsoft Windows HTTP.sys Code Execution Vulnerability
CVE-2015-2051	D-Link DIR-645 Router Series Remote Arbitrary Command Execution Vulnerability
cve-2016-0021	Microsoft Office Memory Corruption Vulnerability
CVE-2017-0147	Windows SMB Information Disclosure Vulnerability
CVE-2017-10271	Oracle WebLogic RCE
CVE-2017-12149	Arbitrary code execution via unrestricted deserialization in ReadOnlyAccessFilter of HTTP Invoker
CVE-2017-12611	Apache Struts Remote Code Execution.
CVE-2017-16894	Laravel Remote Command Execution
CVE-2017-5638	Apache Struts2 RCE Vulnerability
CVE-2017-9791	Apache Struts Remote Code Execution.
CVE-2017-9805	Apache Struts2 RCEVulnerability
CVE-2017-9841	Code injection vulnerability in PHPUnit
CVE-2017-9841	Code injection vulnerability in PHPUnit
CVE-2018-0296	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CVE-2018-10561	Dasan GPON Router Authentication Bypass
CVE-2018-10561	Dasan GPON Router Authentication Bypass
CVE-2018-10562	Dasan GPON Router Remote Command Injection
CVE-2018-11776	Apache Struts 2 Namespace Vulnerability.
CVE-2018-1273	RCE with Spring Data Commons
CVE-2018-13379	An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.
CVE-2018-20062	ThinkPHP 5.0.23 Remote Code Execution
CVE-2018-4901	Adobe Acrobat and Reader APSB18-02 Remote Code Execution Vulnerability
CVE-2018-7490	uWSGI PHP Plugin directory traversal
CVE-2018-7600	Drupal Remote Code Execution
CVE-2018-9126	DotNetNuke DNNarticle Directory Traversal

CVE-2019-0232	Exploit Remote Code Execution (RCE) in CGI Servlet – Apache Tomcat on Windows
CVE-2019-1224	Information disclosure vulnerability in Windows RDP server
CVE-2019-1653	Cisco RV320/RV325 Router Unauthenticated Configuration Export Vulnerability
CVE-2019-16759	vBulletin Pre-Auth RCE Vulnerability
CVE-2019-18935	.NET deserialization vulnerability in the RadAsyncUpload function.
CVE-2020-0688	Microsoft Exchange Validation Key Remote Code Execution Vulnerability
CVE-2020-10148	SolarWinds Orion API authentication bypass and RCE
CVE-2020-10987	Remote Code Execution in Tenda AC15 AC1900
CVE-2020-14882	unauthenticated remote code execution in Oracle WebLogic
CVE-2020-15505	Unauthenticated Remote Code Execution
CVE-2020-17496	vBulletin remote command execution
CVE-2020-25078	D-Link DCS-2530L IP Camera Authenticated Command Injection and Unauthenticated Credential Disclosure
CVE-2020-28188	TerraMaster TOS makecvs.php os command injection
CVE-2020-5902	F5 BIG-IP Traffic Management User Interface code injection
CVE-2020-8958	Guangzhou 1ge Onu/v2804rgw Boaform/admin/formping Dest Ip Address Os Command Injection
CVE-2020-9376	D-LINK DIR-610 GETCFG.PHP INFORMATION DISCLOSURE
CVE-2021-21972	VMware vCenter Unauthorized Remote Code Execution.
CVE-2021-24085	Microsoft Exchange Server Spoofing Vulnerability
CVE-2021-26084	Confluence Server Webwork OGNL injection
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-28141	Unauthorized access to Progress Telerik UI for ASP.NET AJAX 2021.1.22
CVE-2021-28141	unauthorized access for Telerik UI for ASP.NET
CVE-2021-28169	Jetty Utility Servlets Double Decoding Information Disclosure Vulnerability
CVE-2021-3129	Ignition 2.5.1 Remote Code Execution
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-41773	Apache HTTP Server 2.4.49 Path Traversal / Remote Code Execution
CVE-2021-42013	Apache HTTP Server Path Traversal & Remote Code Execution

As the year ends, security professionals have started to address the Log4Shell nightmare and it looks like their troubles have just begun. A transformed work environment with a mixture of remote and hybrid work and an increased trend towards the cloud will further exacerbate the work ahead of us. However, on the bright side are the increased efforts of organisations and security researchers in coming together to share intelligence will help in getting a handle on things. A much-needed push from the governments towards this end is indeed welcome as are the multitude of guidance and availability of resources needed to address rapidly evolving threat scenarios.

About Sequretek

Sequretek is a global cybersecurity company which offers end-to-end security in the areas of enterprise threat monitoring, incident response, device security, identity & access governance through our own AI driven Percept Cloud Security Platform.



Take Control of your enterprise security

- Enterprise scale, easy to use and cloud native
- AI driven threat detection, protection, remediation and response
- Quick implementation and integration capabilities
- End-to-End ownership and management of Sequretek products
- Reduce Total Cost of Ownership (TCO) while simplifying security

Feel free to reach out at info@sequretek.com to know more about our products or to see a live demonstration of our products

TLP: GREEN