Supply Chain Compromise Trends, 2021

Fusion (FS) | Strategic (ST)

April 05, 2022 10:05:00 AM, 22-00005356, Version: 2

Executive Summary

- Mandiant Threat Intelligence identified evidence of more supply chain compromise incidents in 2021 than any year previously examined, though use of this tactic remains uncommon.
- Mandiant identified state-sponsored incidents likely intended to support strategic intelligence collection missions. We attribute most observed incidents to China.
- We noted an increase in financially motivated supply chain compromises, including incidents potentially leading to ransomware.
- For the first time in 2021, we identified more supply chain compromises involving developer tools or software dependencies than traditional software supply chain compromises, which typically target a final product.
- Following several impactful incidents and disclosures, government and technology organizations have taken steps and issued recommendations that we anticipate will increase the difficulty of software supply chain compromises in the medium to long term.

Threat Detail

New Version Details

Version 2, April 5, 2022: Updated text to include FIN7 incident.

Mandiant Threat Intelligence identified more supply chain compromise incidents in 2021 than any year previously examined, though use of this tactic remains uncommon compared to other initial access vectors. Malicious code was added to programs for cryptocurrency trading, biometric authentication, e-government, as well as to open-source libraries and packages used as dependencies in a variety of other software. We noted an increase in financially motivated supply chain compromises, including incidents potentially leading to ransomware.

FIIP ENVIRONMENTS ORGANIZATION
german.simkin@fireeye.com

Figure 1: 2021 supply chain compromise infographic

Supply chain compromise is a particularly dangerous tactic because it abuses the inherent trust that users and enterprise administrators place in hardware, software, and updates supplied by reputable vendors as well as the trust they may not realize they are placing in collaborative code-sharing communities. This tactic also provides tactical and operational advantages to attackers compared to direct targeting. For a variety of malicious actors, the decreased likelihood of detection, as well as the efficiency gain of potentially infecting many victims through one compromise, makes supply chain compromises attractive.

Definition and Methodology

This report describes a specialized subset of third-party compromise: hardware and software supply chain compromise (19-00009070). We define supply chain compromise (T1195) as a situation in which an attacker gains unauthorized access to legitimate infrastructure or tools and implants malicious code or components to be delivered by the

legitimate vendor or repository via the same trusted distribution methods that users would normally employ to obtain the legitimate device, program, package, or update.

We identified incidents through our own collections and/or open-source reporting. This data set is likely not comprehensive; supply chain compromises can be difficult to detect, and there may be an incentive for compromised organizations to underreport them. In some cases, these incidents are not discovered or fully understood until after the fact. However, we believe that this data can still be useful for assessing trends in supply chain compromise. For the full list, please see the Appendix.

While the focus of this research is 2021, it builds upon analysis of supply chain compromise incidents that occurred from 2013–2020, and in some cases includes this data in year-over-year analysis (19-00004036, 21-00010407). We also included 2022 cases identified to date in the Appendix, and referred to these examples where appropriate, but we did not include these incidents in quantitative trend analysis because the full year's data is not yet available.

Supply Chain Compromise Trends

Mandiant identified 31 supply chain compromises in 2021 (Figure 2). This figure reflects continued growth in use of this tactic as an initial compromise vector, though it remains rare overall.

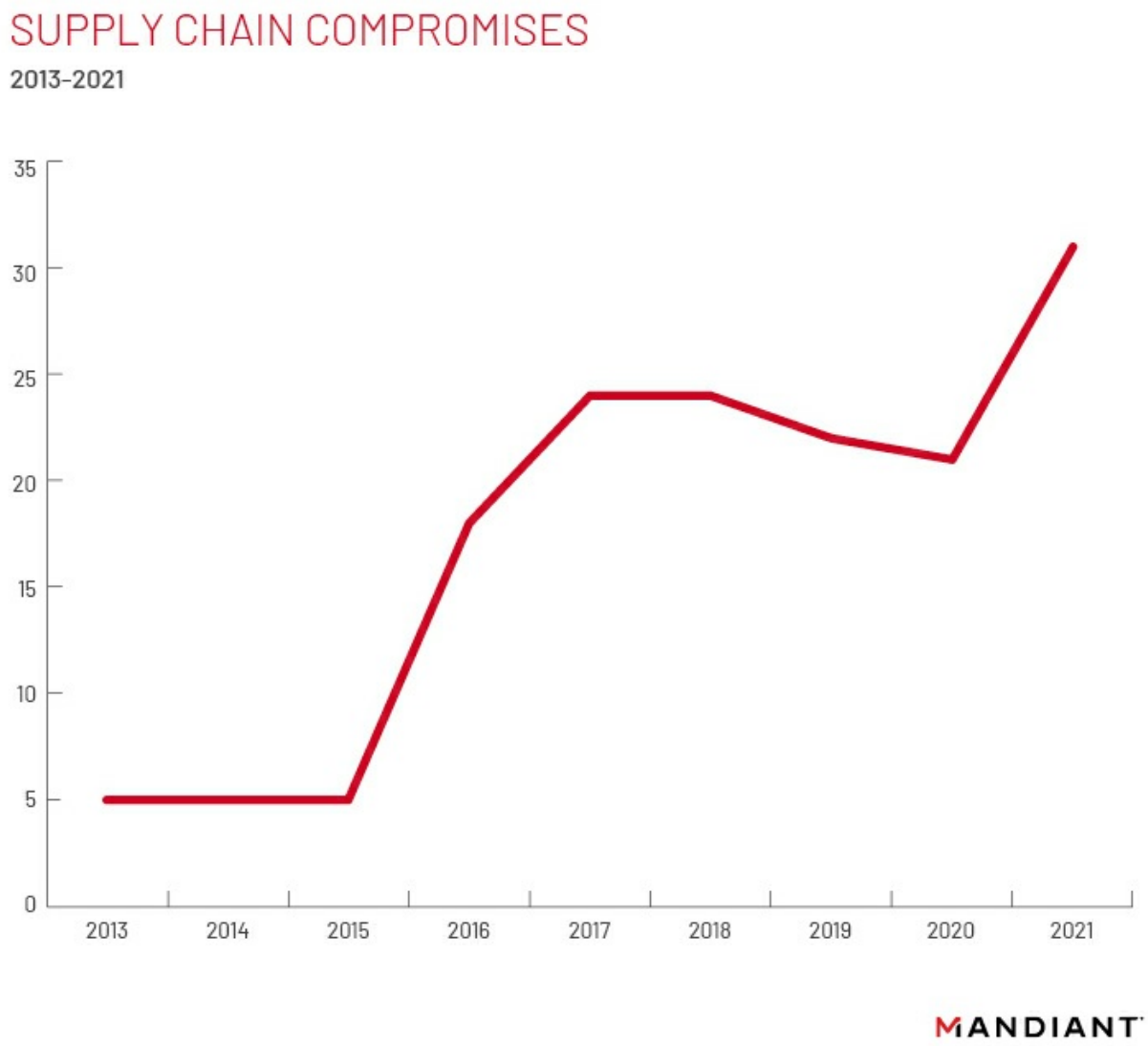

Figure 2: Supply chain compromises, 2013–2021

Supply Chain Compromises by Suspected Motivation

We noted a marked increase in financially motivated supply chain compromises in 2021 and continued to observe suspected cyber espionage incidents in 2021 at approximately the same frequency as the past several years (Figure 3).

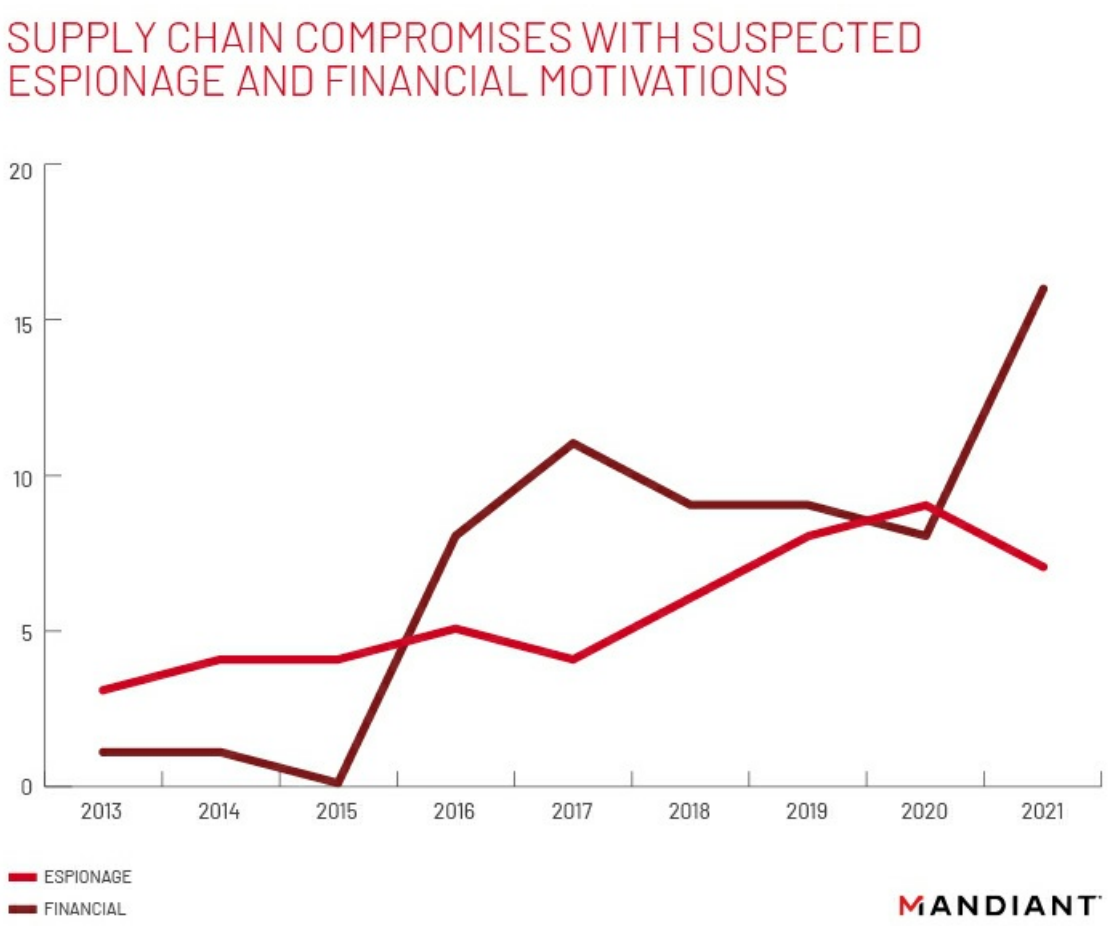

Figure 3: Supply chain compromises with suspected espionage and financial motivations

Supply Chain Compromises Linked to State-Sponsored Actors

Most state-sponsored supply chain compromises that Mandiant identified in 2021 were linked to China. We also observed evidence of potential North Korean and Turkish incidents.

- Continuing a trend from 2019 and 2020, Chinese threat groups implanted malicious code into government software, including a biometric fingerprint scanning program used by a South Asian government and the Mongolian certificate authority MonPass, likely to support intelligence collection efforts in those countries.
- In a similar manner, the reported StrongPity compromise of a Syrian e-government app is consistent with a regional strategic intelligence-gathering effort.
- A trojanized Chrome browser update was likely distributed in China to support domestic monitoring. Censorship programming installed on devices manufactured in China also likely reflects an internal collections mission.
- The UNC251 compromise of the BitGet client installer may represent activity conducted for personal financial gain, rather than a state-directed action. We suspect that this actor conducts threat activity for cyber espionage as well as financial gain, and we have previously observed this actor conduct operations similar to supply chain compromises; for example, using attacker-controlled websites to distribute trojanized versions of Adobe Flash Player and a fake chat app (21-00023993).

Date	Suspected Sponsor	Actor	Trojanized Software	Malware
2021	China	Possibly TEMP[.]Hex	Biometric fingerprint scanning software	SOGU
2021	China	Possibly UNC2263	Mongolian certificate authority MonPass	BEACON
2021	China	UNC3223 (Suspected APT41)	Firefox browser update	SICKMAN, KEYPLUG
2021	North Korea		Latvian IT asset monitoring software	
2021	Suspected Turkey	StrongPity	Syrian e-government Android app	Possibly RUDEBOY
2021	China		Censorship software pre-installed on smartphones manufactured in China	
2022	China	UNC251	BitGet cryptocurrency client installer	OFFRIDER

Table 1: Supply chain compromises linked to state actors

Financially Motivated Supply Chain Compromises

In 2021, Mandiant observed financially motivated actors associated with prior ransomware deployment use software supply chain compromise. We saw this tactic deliver cryptocurrency miners and banking trojans. We also noted open-source reports describing tainted packages and mobile applications used to facilitate cryptocurrency theft and mining, ad fraud, and enrolling users in premium service subscriptions. For more details, please see the Appendix.

- A Mandiant incident response engagement revealed that a malicious actor trojanized an installer for CCTV software hosted on a legitimate website likely in May 2021. Upon installing the software, a chain of downloads and scripts were executed, leading to SMOKEDHAM and later NGROK on the victim's computer. We attribute this activity to UNC2465, one of several activity clusters known to conduct ransomware and data theft extortion operations (21-00013736). Mandiant discovered that in February 2022,

UNC2465 again compromised the same CCTV camera website to redirect download links for its software to deliver a malicious installer that deploys SMOKEDHAM (22-00004162).
- In late 2021, FIN7 compromised a website that sells digital products and modified multiple download links to point to an Amazon S3 bucket hosting trojanized versions containing an Atera agent installer. This remote management tool was later used to deploy POWERPLANT to the victim system (22-00008217).
- The chief technology officer (CTO) of the SushiSwap decentralized finance (DeFi) company reported an apparent insider threat scenario in which a contractor with access to the organization's MISO platform GitHub repository published a malicious commit replacing the wallet address for an auction on the platform with his personal address. After successfully diverting the auction proceeds, the attacker apparently returned the funds.
- In two separate incidents in October and November 2021, we identified that malicious code had been inserted into popular npm packages coa, rc, and UAParser[.]js that would lead to the distribution of malware including coinminers and DANABOT instances associated with botnet ID 40. We are tracking this activity as UNC3379 (21-00023166, 21-00023971). UAParser[.]js is reportedly downloaded 6 to 7 million times a week and is used by many high-profile companies. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert about the compromise.

We anticipate that financially motivated supply chain compromises could continue to expand in both quantity and impact based on observed growth, increased public attention, use of this tactic in the FIN7, SMOKEDHAM, and DANABOT incidents, and the increasing professionalization and skill specialization of cyber crime operations (21-00012276).

- In addition to outright compromise, there are reportedly companies using financial incentives to encourage open-source developers to cede control of their content or incorporate third-party code in a manner similar to insider threat activity. Brian Krebs described an ecosystem in which companies offer to buy popular browser extensions or compensate the developers, who typically do not recognize revenue from extensions, for including the company's code in the extension.

Supply Chain Compromises Introduced via Third-Party Resources, Developer Tools

For the first time in 2021, we identified more supply chain compromises involving developer tools or software dependencies (T1195.001) than compromises affecting final software products (T1195.002) (Figure 4).

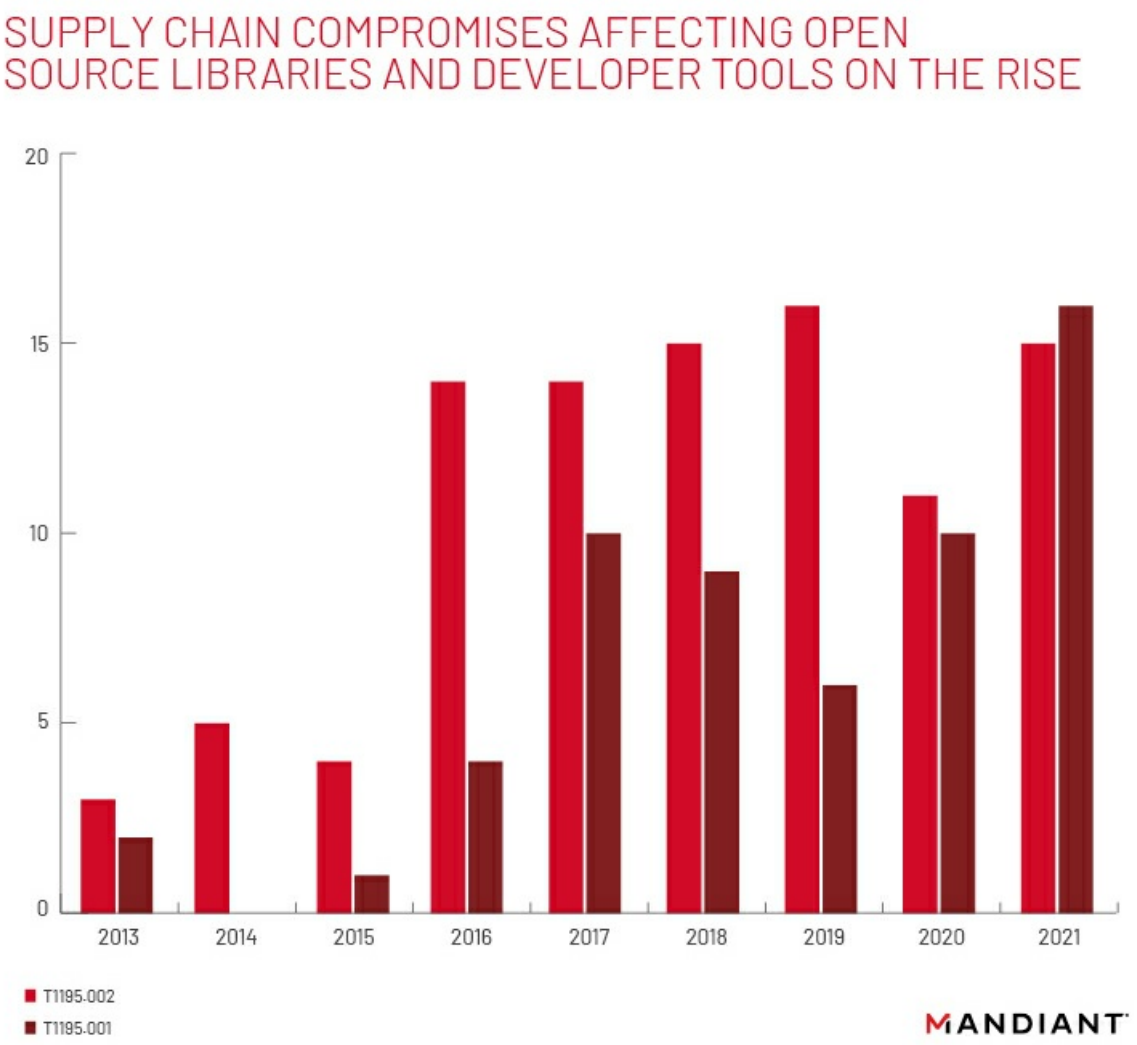

Figure 4: Supply chain compromises affecting developer tools and software dependencies on the rise

These incidents frequently involved resources from open-source or collaborative communities, such as libraries and other code packages from PyPI or npm, Docker virtualization images, and WordPress plugins and themes, and often sought to collect environmental variables, credentials, and deploy coinminers. We also noted examples of actors abusing open-source repositories to spread protest messages.

- In March 2021, Palo Alto researchers discovered 30 malicious Docker images that had been downloaded from Docker Hub a combined 20 million times, and by tracing cryptocurrency wallet addresses and mining pool credentials, estimated that the operation had netted the attackers the equivalent of $200,000 USD (21-00007111).
- The UNC3379 DANABOT incidents, described above, targeted popular npm packages to distribute malicious code.
- Researchers identified malicious npm packages typosquatting noblox[.]js, an open-source JavaScript API for the Roblox game. The malicious packages contain a number of components, including to steal Discord and other credentials stored in the browser, to repeatedly open pop-up alerts reading "run away," and to deploy "Monster" ransomware.
- In the weeks after Alex Birsan's dependency confusion blog was published, a suspected vigilante using the username "RemindSupplyChainRisks," uploaded more

than 3,500 packages to PyPI and more than 1,500 to npm to call additional attention to supply chain risks. While examined packages appeared to be benign, they did use names that closely resembled commonly used packages.
- In March 2022, the developer of the npm node-ipc JavaScript library intentionally introduced malicious functionality in response to the Russian invasion of Ukraine. The update would check to see if the host machine was located in Russia or Belarus, and if so, it would overwrite or wipe data and display a message "calling for world peace." Subsequently released versions remove the destructive functionality but distribute text files containing anti-war statements.

Additionally, we identified several more significant incidents targeting foundational elements of enterprise software development as well as web and mobile internet browsing.

- Codecov, which offers software auditing tools and a platform host code testing reports and statistics, disclosed that an unknown threat actor managed to modify its Bash Uploader script. According to Codecov, "…beginning January 31, 2021, there were periodic, unauthorized alterations of our Bash Uploader script by a third-party, which enabled them to potentially export information stored in our users' continuous integration (CI) environments. This information was then sent to a third-party server outside of Codecov's infrastructure" (21-00008591). Subsequently, several companies disclosed potential exposure of credentials and source code as a result of the Codecov compromise (21-00010940).
- PHP maintainer Nikita Popov confirmed that in March 2021, threat actors pushed two malicious commits to the PHP source code repository, suggesting that the attackers may have compromised the repository's server in order to upload malicious code containing a backdoor. Open sources claim that PHP supports the function of approximately 80 percent of websites on the internet (21-00006975).
- European academic researchers found that the GEA-1 and GEA-2 encryption algorithms used to encrypt 2G and 3G mobile GPRS internet traffic were deliberately weakened. The European Telecommunications Standards Institute (ETSI), which developed GEA-1, confirmed that the algorithm was weakened to satisfy export requirements at the time. The research suggests that mobile internet traffic relying on these algorithms could be decrypted and passively intercepted. While use of these algorithms was most common from 2000–2010, an attacker could trick modern devices that still support the older protocols to fall back to the vulnerable encryption.

No Hardware Supply Chain Compromise Observed, but Reports of Pre-Installed Malware Noted

We did not find evidence of hardware supply chain compromise (T1192.003) incidents in 2021. We did find accounts of mobile and other devices shipped with malware or apps with excessive permissions pre-installed.

- German users reported significant issues with Gigaset Android devices beginning in March 2021 resulting in pop-up ads, social media account takeover, and fraudulent messages. Malwarebytes reports that a pre-installed system application "Update" will install multiple malicious applications that attempt to install additional malicious applications from gaming websites and send WhatsApp and SMS messages prompting

other users to install malware. The issue also apparently affected Siemens and Alps devices. Gigaset reported that malicious actors compromised a server belonging to its third-party update service provider.
- In September 2021, the Lithuanian National Cyber Security Center (NCSC) warned that pre-installed apps including the browser of Xiaomi-made Mi 10T smartphones contained capabilities to censor phrases such as "Free Tibet." Although this capability is disabled on devices sold in Europe, it could be activated without user knowledge.
- In October 2021, the U.S. Federal Bureau of Investigation (FBI) reportedly raided a warehouse located in Florida belonging to China-based payment terminal maker PAX Technology over speculation that its terminals contain pre-installed malware. Reports suggest that the PAX terminals were allegedly being used as malware droppers and command and control (C&C) locations for staging attacks and stealing data. According to security researcher Brian Krebs, the raid may be related to incidents in the U.S. and EU that were reported by a large U.S. payment processor that found their machines were displaying suspicious behavior and allegedly emanating unusual network packets whose sizes did not match the data they should have been sending (21-00023331).

Increased Scrutiny on Software Supply Chain and Dependency Risk

The SUNBURST incident, discovered in late 2020, drew significant additional public attention to software supply chain risk (21-00004396). Subsequent research and incidents, including Alex Birsan's February 2021 "Dependency Confusion" blog and the CVE-2021-44228 Log4j vulnerability exploitation campaign beginning in December 2021, underscore the additional risk posed by malicious actor abuse of open-source software repositories (21-00026727).

Government authorities and technology organizations have responded with several initiatives and studies seeking to reduce software supply chain and software dependency risk.

- U.S. President Biden issued a cybersecurity executive order in May 2021, which included directives to NIST to research and provide guidelines for improving supply chain security. The order also directed the U.S. government to move toward a zero trust architecture.
    - Mandiant believes that trends in business operations, such as integration of third-party vendors and use of cloud hosting, as well as adversary behavior targeting third parties and the software supply chain highlight the advantages of a zero trust security model (21-00011773).
- In October 2021, the U.S. House of Representatives passed the DHS Software Supply Chain Risk Management Act of 2021. This legislation is intended to reduce software supply chain risk for the Department of Homeland Security (DHS) by requiring contractors to submit a software bill of materials (SBOM) and attest to the lack of defects or vulnerabilities in code provided to the department.
- A European Union Agency for Cybersecurity (ENISA) study noted the growing risk of supply chain compromise due to the increasingly interconnected nature of enterprise operations, and recommended increased vigilance by both customers and suppliers to minimize opportunities for a security failure.

- Google and the Open-Source Security Foundation released OpenSSF Security Scorecards in fall 2020, with an update in summer 2021. The scorecard project seeks to provide an automated test that will quickly produce a security assessment, or score, of an open-source project.
- Academic research from Microsoft and North Carolina State University released in December 2021 identified six key indicators of security weakness in npm packages to provide developers and security researchers with potential clues to identify, predict, and prevent software supply chain compromises.
- In December 2021, npm announced that it would implement enhanced verification measures, including enrolling all npm publishers in mandatory two-factor authentication, by March 2022.

Mandiant anticipates that increased scrutiny on the issue and the implementation of these measures will increase the difficulty of supply chain compromises where these regulations and policies can be enforced in the medium to long term. However, we also expect that the tactical and operational advantages will continue to encourage attackers to attempt supply chain compromises, and the trendline (Figure 2) indicates steady growth since 2013. Further, particularly skilled and well-resourced attackers will likely continue to attempt supply chain compromises against enterprise software and/or outside of the potential jurisdiction of these regulations.

Mitigation Recommendations

By design, supply chain compromises are difficult to detect and prevent. We suggest that organizations contemplate applying multiple layers of security policies, plans, and solutions to maximize opportunities to prevent and detect an anomaly or compromise.

To mitigate risk from potential supply chain compromises affecting enterprise software and hardware solutions from outside providers, organizations may consider:

- Establishing a vendor vetting process to evaluate vendor security practices prior to deploying hardware or software. Part of this evaluation process may include verifying compliance attestations from third-party auditors, reviewing the vendor's privacy program, as well as implementing repair/replacement parts management process and counterfeiting detection elements for hardware components.
- Establishing a change control process and board for all enterprise hardware and software changes, which could include a centralized IT or IT security managed process for downloading, testing, and pushing updates out to users.
- Using an advanced endpoint security solution, such as an endpoint detection and response (EDR), to detect malicious behavior if a tainted software package is downloaded and executed.
- Ensuring proper logging and monitoring is in place between the software/hardware and the internet.
- Implementing the software/hardware using network segmentation with minimal access to the internet. For example, if SolarWinds Orion lacked internet access, it would not have been able to communicate to the C&C.

To mitigate the risk of potential supply chain compromises linked to internal employees

inadvertently incorporating malicious libraries or packages from third-party resources into software developed internally, organizations might consider:

- Establishing formal policies encouraging security best practices, including security audits of code in development.
- Supporting training programs to assist employees in following these best practices.
- Instituting network segmentation to isolate development environments.
- Using advanced network and endpoint security solutions to detect malicious behavior in the event of a compromise.
- Establishing an IT or IT security managed process to examine and approve open-source packages requested by users. Make approved versions available to employees in a repository.

Formal Software Development Lifecycle: Security assessments and audits should be an integral part of the software development lifecycle or continuous integration and deployment (CI/CD) pipeline for any internally developed software that is customer facing or integral to internal functions of the organization. Given attacker interest in compromising developer tools, and the significant downstream implications for software providers, it could be beneficial for IT security teams to give special attention to procurement, subscriptions, and updates to tools used to build an organization's software.

Informal Software Development: If users at your organization engage in informal script or tool development, setting up a segmented environment to host these experimental tools, as well as establishing formal policies and training programs to reinforce best practices (including security testing) may help to offset risk.

Appendix: Supply Chain Compromise Incidents, January 2021 to February 2022

2021

Date	Incident
January 2021	In January 2021, open-sources claimed that GeoBook 1E laptops shipped to British schools to support remote learning arrived with the Gamarue remote access trojan (RAT) pre-installed.
January 2021	Codecov, which offers software auditing tools and a platform host code testing reports and statistics, disclosed that an unknown threat actor managed to modify its Bash Uploader script. According to Codecov, "...beginning January 31, 2021, there were periodic, unauthorized alterations of our Bash Uploader script by a third-party, which enabled them to potentially export information stored in our users' continuous integration (CI) environments. This information was then sent to a third-party server outside of Codecov's infrastructure" (21-00008591). Subsequently, several companies have disclosed potential exposure of credentials and source code as a result of the Codecov compromise (21-

	00010940).
February 2021	Avast reported that Mongolian certificate authority MonPass was compromised in early 2021, and as part of this compromise, the MonPass client available for download from the legitimate website included a backdoor from early February to early March 2021. According to the researchers, the execution chain also involved stenography; in addition to downloading the legitimate installer, the backdoored client would also download an image in the background that contained an encrypted BEACON sample. This campaign shares IOCs with activity we track as UNC2263, which has previously targeted Hong Kong. Targeting of Hong Kong and Mongolia provides some indication that the operation is the work of a Chinese espionage actor (21-00014857).
February 2021	Software testing company Qentinel reported that three packages using names of packages included in the company's software testing tool had been uploaded to PyPI by an unknown actor. The presence of these packages on PyPI caused the organization's build pipelines to fail because its code requested these third-party packages, rather than internal libraries that contained necessary functionalities. This compromise scenario was also outlined in Alex Birsan's Dependency Confusion blog. Unless a user specifies the URL of an internal repository in their request, a pip request will fetch packages from the public PyPI repository. Qentinel did not find evidence of malicious functionality in the third-party packages and worked with PyPI to have them removed and the names blocklisted to prevent future incidents.
February 2021	Mandiant research identified a legitimate South Asian government website distributing a biometric fingerprint scanning software used by government employees that had been packaged with SOGU. We believe the trojanized version was available for download from February to at least June 2021. Kaspersky reporting likely also describes this activity, which it attributes to Chinese cyber espionage group "HoneyMyte."
March 2021	In the weeks after Alex Birsan's dependency confusion blog was published, a suspected vigilante using the username "RemindSupplyChainRisks" uploaded more than 3,500 packages to PyPI and more than 1,500 to npm to call additional attention to supply chain risks. While examined packages appeared to be benign, they did use names that closely resembled commonly used packages.
March 2021	PHP maintainer Nikita Popov confirmed that in March 2021, threat actors pushed two malicious commits to the PHP source code repository, suggesting that the attackers may have compromised the repository's server in order to upload malicious code containing a backdoor. Open sources claim

	that PHP supports the function of approximately 80 percent of websites on the internet (21-00006975).
March 2021	In March 2021, Palo Alto researchers discovered 30 malicious Docker images that had been downloaded from Docker Hub a combined 20 million times, and by tracing cryptocurrency wallet addresses and mining pool credentials, estimated that the operation had netted the attackers the equivalent of $200,000 USD (21-00007111).
April 2021	In April 2021, Australian software provider Click Studios disclosed that malicious actors had compromised the update mechanism for its password management software Passwordstate (21-00009348). Danish cyber security firm CSIS examined the incident and claimed that the update package contained a malicious DLL dubbed "mouserpass."
March 2021	German users reported significant issues with Gigaset Android devices beginning in March 2021 resulting in pop-up ads, social media account takeover, and fraudulent messages. Malwarebytes reports that a pre-installed system application "Update" will install multiple malicious applications that attempt to install additional malicious applications from gaming websites, send WhatsApp and SMS messages prompting other users to install malware. The issue also apparently affected Siemens and Alps devices. Gigaset reported that malicious actors compromised a server belonging to its third-party update service provider.
March 2021	A March 2021 software update for the popular third-party Android appstore APKPure's client reportedly contained an advertisement SDK that included the Triada trojan.
April 2021	Researchers identified a set of PyPI packages typosquatting other popular packages that would deliver the "Ubqminer" coinminer. The malicious packages, mostly using variations of the name *maratlib*, had reportedly been downloaded nearly 5,000 times.
April 2021	Researchers discovered the npm package *web-browserify* typosquatting the legitimate, popular package *browserify*, which contains a malicious Linux and Mac executable packaged along with hundreds of legitimate components. The malware performs a number of reconnaissance and privilege escalation tasks, establishes persistence, and attempts to wipe the /etc/ directory. The researchers assess that the package appears to specifically be targeting NodeJS developers.
May 2021	A Mandiant incident response engagement revealed that a malicious actor trojanized an installer for CCTV software hosted on a legitimate website likely in May 2021. Upon installing the software, a chain of downloads and scripts were executed, leading to SMOKEDHAM and later NGROK on

	the victim's computer. We attribute this activity to UNC2465, one of several activity clusters known to conduct ransomware and data theft extortion operations using DARKSIDE (21-00013736).
May 2021	TrendMicro described a campaign in which malicious actors apparently gained unauthorized access to a Syrian government website and replaced a legitimate Syrian e-government Android application with a version that had been packaged with a backdoor in May 2021. TrendMicro attributes the activity to StrongPity.
May 2021	In September 2021, Mandiant Threat Intelligence identified trojanized Google Chrome updaters dubbed "SICKMAN," which result in the KEYPLUG backdoor. A SICKMAN loader was contained within a fake Firefox installer and hosted on a website masquerading as a legitimate Mozilla site. While victimology is unclear, accessing the fake Mozilla site will lead to the Chinese version of the Mozilla website, suggesting the possibility of internal targeting that could expand to Chinese diaspora abroad. Further, SICKMAN loader naming conventions and infrastructure hint that the actor is masking the campaign as a possible browser update, which can appeal to a wider audience. Infrastructure for this campaign dates to at least May 2021, indicating it is an ongoing and likely successful campaign. We currently track this activity as UNC3223 but note potential ties to APT41 (21-00021921).
June 2021	European academic researchers found that the GEA-1 and GEA-2 encryption algorithms used to encrypt 2G and 3G mobile GPRS internet traffic were deliberately weakened. The European Telecommunications Standards Institute (ETSI), which developed GEA-1, confirmed that the algorithm was weakened to satisfy export requirements at the time. The research suggests that mobile internet traffic relying on these algorithms could be decrypted and passively intercepted. While use of these algorithms was most common from 2000–2010, an attacker could trick modern devices that still support the older protocols to fall back to the vulnerable encryption.
June 2021	Kaspersky reported that it observed North Korean actors conduct two supply chain compromises, including one involving a South Korean security software, and the other via a Latvian asset monitoring company. Mandiant cannot independently confirm these compromises (21-00023462). The South Korean security software example may be referring to the WIZVERA VeraPort example described by ESET in November 2020 (20-00023605), though the reported June timeline might better match CHOCOLATEPIE, an Android application Mandiant identified disguised as a South Korean

	government anti-virus product (21-00010402). We did not identify a delivery method in this case and cannot confirm that the .apk was hosted on a legitimate website or by a legitimate source.
July 2021	Researchers identified eight malicious PyPI packages that are designed to perform a variety of functions. Six of the packages conduct device reconnaissance and steal Discord authentication tokens as well as credit card numbers and passwords stored in a browser. Two of the packages attempt to execute code hosted at a private IP address. The packages had reportedly been downloaded approximately 30,000 times (21-00016965).
September 2021	The chief technology officer (CTO) of the SushiSwap decentralized finance (DeFi) company reported that a contractor with access to the organization's MISO platform GitHub repository published a malicious commit replacing the wallet address for an auction on the platform with his personal address. After successfully diverting the auction proceeds, the attacker apparently returned the funds.
September 2021	The Lithuanian National Cyber Security Center (NCSC) warned that pre-installed apps including the browser of Xiaomi-made Mi 10T smartphones contained capabilities to censor phrases such as "Free Tibet." Although this capability is disabled on devices sold in Europe, it could be activated without user knowledge.
September 2021	Researchers reported that malicious actors compromised the website of AccessPress, a WordPress themes and extensions vendor, and added a PHP backdoor to 93 themes and extensions provided by this vendor. Sucuri analysis suggests that the malicious actors used the backdoors to resell access to websites running malicious versions of AccessPress themes and extensions.
September 2021	Open sources reported that at least four models of low-cost phones sold in Russia arrived from manufacturers with malware pre-installed that would subscribe users to premium SMS services.
October 2021	Sonoatype identified that malicious npm libraries *klow* and *klown*, which were used as dependencies for additional npm packages using variations of the name *okhsa*, contain cryptocurrency miners. The packages were reportedly only live for one day before npm removed them.
Late 2021	FIN7 compromised a website that sells digital products and modified multiple download links to point to an Amazon S3 bucket hosting trojanized versions containing an Atera agent installer. This remote management tool was later used to deploy POWERPLANT to the victim system. This was the first time Mandiant observed FIN7 leverage supply chain

	compromise (22-00008217).
October 2021	Malicious actors gained unauthorized access to the npm account belonging to Faisal Salman, the developer of the popular UAParser[.]js JavaScript library, and used this access to publish versions embedded with malware. Mandiant identified multiple cases in the wild where subverted UAParser[.]js packages led to the distribution of malware including coinminers and instances of DanaBot associated with botnet ID 40 and is tracking this activity as UNC3379. The malicious code in identified cases would execute a shell or batch script depending on whether the impacted host was running Linux or Windows and would ultimately download malware via either curl, wget, or certutil (21-00023166). UAParser[.]js is reportedly downloaded 6 to 7 million times a week and is used by many high-profile companies. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert about the compromise.
October 2021	The U.S. Federal Bureau of Investigation (FBI) reportedly raided a warehouse located in Florida belonging to Wanchai, Guangdong, China-based payment terminal maker PAX Technology over speculation that its terminals contain pre-installed malware. Reports also indicate that the PAX terminals were allegedly being used as malware droppers and command and control (C&C) locations for staging attacks and stealing data. According to security researcher Brian Krebs, the raid may be related to cyber attacks against the U.S. and EU that were reported by a large U.S. payment processor that found the machines were displaying suspicious behavior and allegedly emanating unusual network packets whose sizes did not match the data they should be sending (21-00023331).
October 2021	Sonatype identified malicious npm packages typosquatting noblox[.]js, an open-source JavaScript API for the Roblox game. Gamers use the legitimate API to write scripts that interact with the Roblox website and game. The malicious packages contain a number of components, including to steal Discord and other credentials stored in the browser, to repeatedly open pop-up alerts reading "run away," and deploy "Monster" ransomware.
November 2021	On Nov. 4, 2021, Mandiant Threat Intelligence observed a compromised NPM package for the "coa" JavaScript library being leveraged to distribute DANABOT payloads with botnet ID 40. On the same day, an alert was published on GitHub indicating that the NPM package rc had versions published with similar malicious code. We believe this activity is related to the October 2021 compromise of UAParser[.]js, and we are tracking this activity as UNC3379 (21-00023971).

November 2021	Researchers from Jfrog reported 11 malicious PyPI packages, including backdoors, packages that would collect environmental data when installed, and several with Discord token-stealing functionality.
December 2021	Independent researcher Andrew Scott identified three malicious PyPI packages, *aws-login0tool*, *dpp-client*, and *dpp-client1234*, typosquatting legitimate packages. The first was flagged in VirusTotal as a trojan and was only available on the PyPI index for 10 days, but it was downloaded at least 600 times before getting removed. The two dpp-client packages were reportedly uploaded by the same user in February 2021, and searched for environmental data, particularly any references to Apache Mesos.
December 2021	Jfrog researchers identified 17 npm packages, which included functionality to collect environmental variables, Discord credential stealers, and packages containing PirateStealer, which would collect Discord credentials along with additional data, including credit card information.

Table 2: 2021 supply chain compromise incidents

2022

Date	Incident
January 2022	Mandiant discovered evidence that the legitimate installer for the Bitget cryptocurrency exchange platform client contained the OFFRIDER malware, which we attribute to a Chinese threat group UNC251. The trojanized installer was hosted on a legitimate domain in January 2022 (22-00001928). We suspect that UNC251 conducts threat activity for cyber espionage as well as financial gain, and we have previously observed related threat activity using attacker-controlled websites to distribute trojanized versions of Adobe Flash Player and a fake chat app (21-00023993).
January 2022	In January 2022, the developer of popular npm packages *colors* and *faker* introduced code to these packages to break the original functionality and display an apparent protest message and a string of non-ASCII characters in a loop on any application using the libraries. The developer warned in November 2020 that he did not intend to continue supporting the *faker* package for free.
February 2022	Researchers identified a malicious npm package, *jquery-lh*, typosquatting the popular jQuery project. The package will collect environmental variables and send them to an attacker-controlled server.
	Mandiant discovered that in February 2022, UNC2465 returned to the same CCTV camera website it compromised in May 2021, causing download links for its software to redirect to an

February 2022	installer that would deliver SMOKEDHAM (22-00004162). While the final goal of these operations is unclear, UNC2465's prior use of DARKSIDE suggests that these operations may ultimately result in the deployment of ransomware, albeit an alternative given the closure of DARKSIDE in mid-2021 (21-00010945).
March 2022	In early March 2022, the developer of the popular npm *node-ipc* JavaScript library updated the code, intentionally introducing malicious functionality described as CVE-2022-23812, evidently in response to the Russian invasion of Ukraine. The update would check to see if the host machine was located in Russia or Belarus based on its IP address, and if so, it would overwrite or wipe data and display a message "calling for world peace." Subsequently released versions remove the destructive functionality but distribute text files containing anti-war statements. Notably, node-ipc is included as a dependency in many other libraries, and the wiper and protest components could reportedly affect users who access a web page or application using node-ipc (22-00007242).

Table 3: 2022 supply chain compromise incidents

Please rate this product by taking a short four question survey

First Version Publish Date

March 23, 2022 02:29:00 PM

Threat Intelligence Tags

Affected Industry

- Technology
- Governments
- Financial Services
- Media & Entertainment

Target Geography

- United States of America
- China
- Syria
- Mongolia
- India
- Latvia
- Singapore
- Japan
- Germany
- Lithuania
- United Kingdom

Intended Effect

- Military Advantage
- Political Advantage
- Credential Theft/Account Takeover
- Financial Theft

Affected System

- Users/Application and Software

Motivation

- Financial or Economic
- Ego
- Military/Security/Diplomatic
- Opportunistic

Source Geography

- China
- Turkey
- North Korea

Targeted Information

- Credentials
- Government Information
- Financial Data

Tactics, Techniques And Procedures(TTPs)

- Hardware/Supply Chain Compromise

Actor

- UNC2465
- FIN7

Malware Family

- KEYPLUG
- SOGU
- RUDEBOY
- DANABOT
- BEACON
- NGROK
- SMOKEDHAM
- OFFRIDER
- SICKMAN

Common Vulnerabilities and Exposures

CVE ID: CVE-2021-44228(NVD Description)External Link
CVE-2022-23812(NVD Description)External Link

Version Information

Version:1.0, March 23, 2022 02:29:00 PM
Supply Chain Compromise Trends, 2021

Version:2.0, April 05, 2022 10:05:00 AM
Supply Chain Compromise Trends, 2021

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/22-00005356