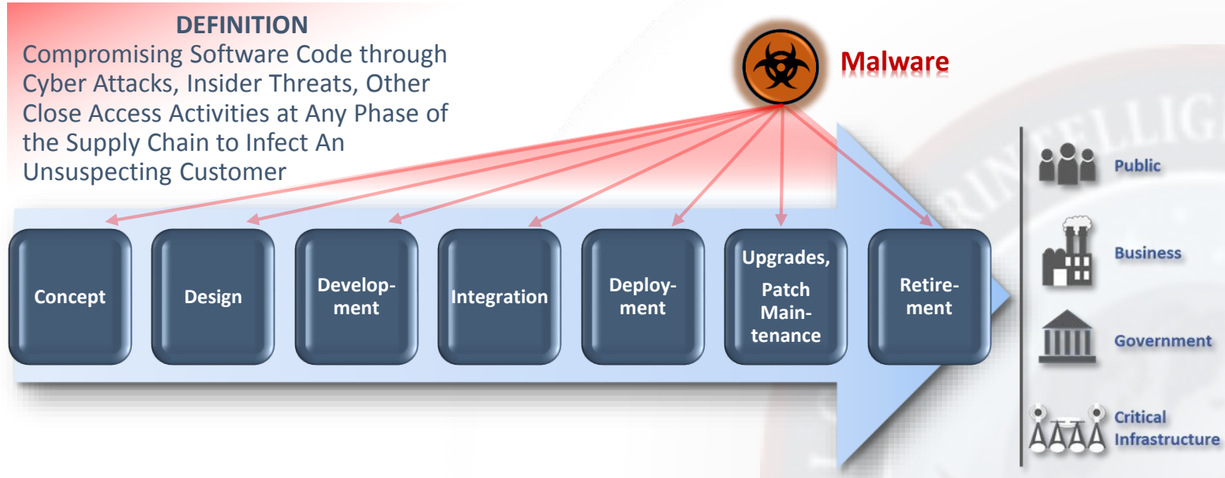
Software Supply Chain Attacks

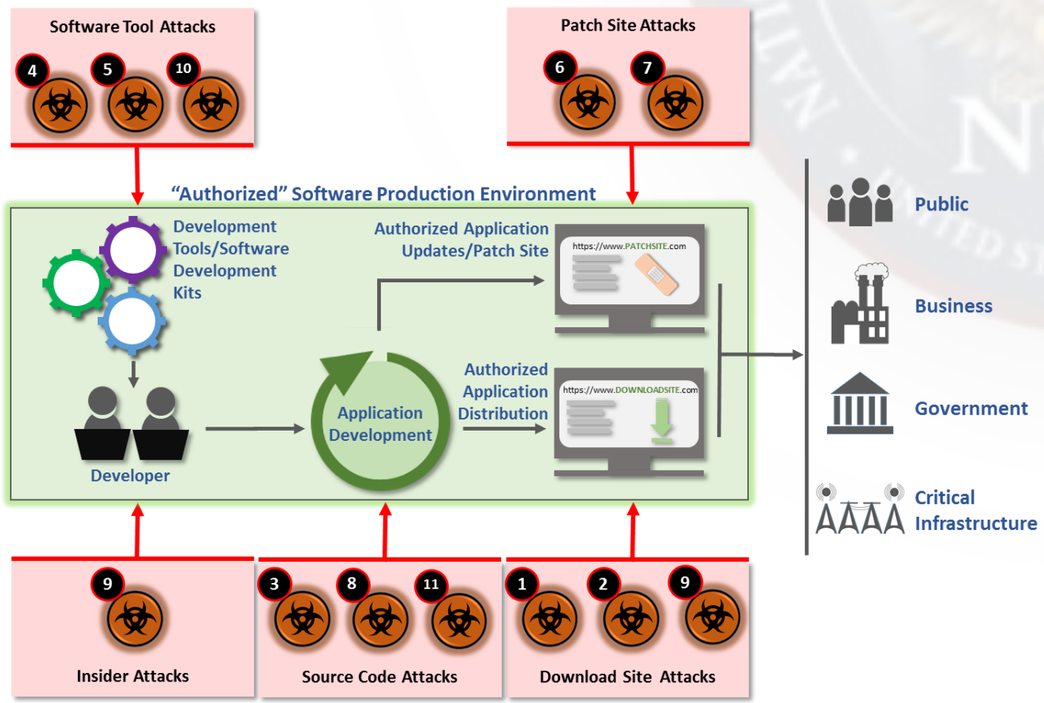
Adversaries Use Attack Campaigns for Extortion, Data Exfiltration, Manipulation and Destruction - Possibly With Strategic Intent

1) What is a Software Supply Chain Attack?

DEFINITION
Compromising Software Code through Cyber Attacks, Insider Threats, Other Close Access Activities at Any Phase of the Supply Chain to Infect An Unsuspecting Customer



2) Proven Vectors From Which Attacks Occur



3) Recent, Prominent Supply Chain Attacks on Software

Software supply chain attacks can be:

- *Simple.* Corrupting a vendor's patch site by placing malware files similarly named to authorized code, in the hopes that the malware file is downloaded. (e.g., Mongose.xxx vs Mongoose.xxx)

OR

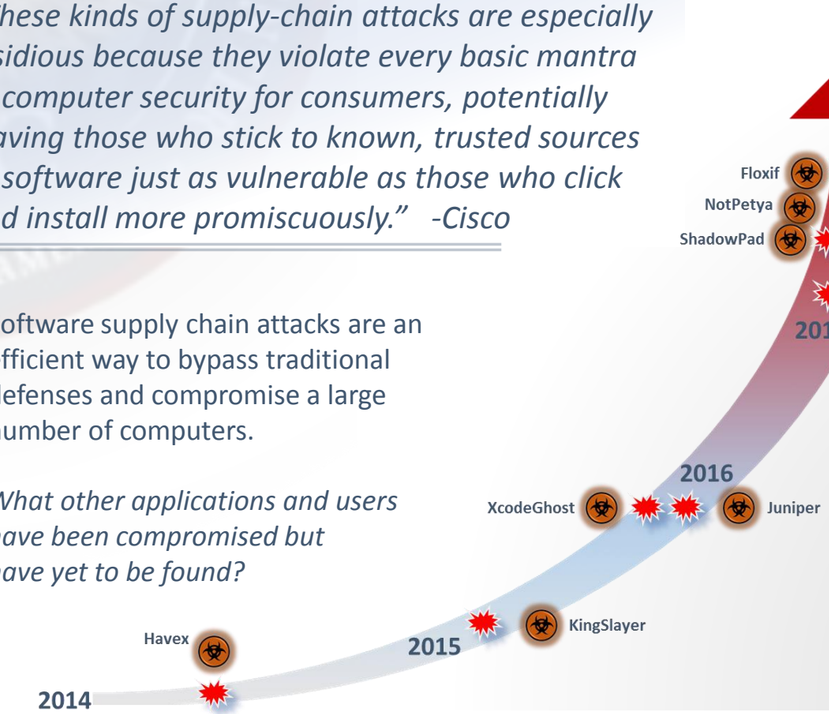
- *Complicated.* Infiltrating the code base to insert malware before the code is compiled or electronically signed.

Legend	Date	Attack Name	Target Technology	Attack Vector	Attack Note
1	Jun 2014	Havex / Dragonfly	Industrial Control Systems	Download Site Attack	• Watering hole attack
2	Apr 2015	KingSlayer	Network Logs and Event Monitor Tools	Download Site Attack	• Subversion at distribution point by redirecting download request to malicious actor site
3	Dec 2015	Juniper Network Attack	Network Equipment Source Code	Source Code Attack	• Unauthorized code added which created authentication bypass and ability to monitor and decrypt VPN traffic
4	Dec 2015	XcodeGhost	iOS	Software Development Tool Attack	• Fake version of the developer tool distributed to site frequented by developers
5	Jan 2017	Expensive Wall / Shady SDK	Android	Software Development Tool Attack	• Obfuscation used by malware developers to encrypt malicious code, allowing evasion of anti-malware protections
6	Jun 2017	Un-Named Attack	Python	Patch Site Attack	• Typosquatting attack
7	Jun 2017	NotPetya	MeDoc	Patch Site Attack	• Software infrastructure compromise to tamper with code
8	Jul 2017	Shadowpad	Network Manage Software Suite	Source Code Attack	• Backdoor injected into a network management software suite then pushed through software update
9	Aug 2017	Floxif	CCleaner	Insider/Download Site Attack	• Infiltration into development or distribution process before cryptographic signature for software occurred
10	Aug 2017	HackTask	JavaScript	Software Development Tool Attack	• Typosquatting attack
11	October 2017	Un-Named North Korea Attack	Anti-Virus Code	Source Code Attack	• Infiltrated network of a company providing computer anti-virus service

4) Is This A Trend?

"These kinds of supply-chain attacks are especially insidious because they violate every basic mantra of computer security for consumers, potentially leaving those who stick to known, trusted sources of software just as vulnerable as those who click and install more promiscuously." -Cisco

- Software supply chain attacks are an efficient way to bypass traditional defenses and compromise a large number of computers.
- *What other applications and users have been compromised but have yet to be found?*



Damage Undetermined

- **CCleaner** – 2.2 million affected
- **NK Attack** – Potential loss of classified South Korean military plans
- **KingSlayer** – At least one defense contractor infected and then targeted

Dated: 30 October 2017

Software Supply Chain Attacks

Compromising Software Through Software Supply Chain Attacks

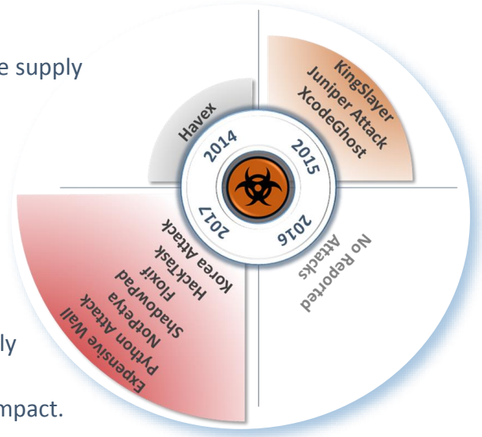
Adversaries Use Attack Campaigns for Extortion, Data Exfiltration, Manipulation and Destruction - Possibly With Strategic Intent

Definition: Compromising software code through cyber attacks, insider threats, and other close access activities at any phase of the supply chain to infect an unsuspecting customer

Hackers are circumventing traditional cyber defenses to compromise software and delivery processes to enable successful, rewarding and stealthy methods to subvert large numbers of computers through a single attack. Cyber experts predicted the use of this attack vector because (1) many software development and distribution channels lack proper cyber and process protections, and (2) other cyber attack paths become less optimal as system owners improve the overall cybersecurity posture of their networks, components and computers. Adversaries can use these generalized attacks to target specific victims to conduct extortion campaigns or exfiltrate, manipulate or destroy data for some targeted, deliberate purpose.

Attacks and Impacts Are Expanding.

2017 has represented a watershed year in the reporting of software supply chain attacks. So far in 2017, seven significant events have been reported in the public domain compared to only four between 2014 – 2016. These numbers may not represent all significant attacks that occurred as malware injected into software code is difficult to detect; discovery may not occur until well in the future.



While the numbers of attacks are growing, so too are the potential impacts. Hackers are clearly targeting and attacking software supply chains to achieve some desired effect, e.g., cyber espionage, intentional disruption to organizations, or demonstrable financial impact.

- *Floxif / CCleaner:* Floxif infected 2.2 million worldwide CCleaner customers with a backdoor. Attackers specifically targeted 18 companies and infected 40 computers to conduct espionage to gain access to Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.
- *Attack on South Korea:* Hackers compromised a commercial anti-antivirus package to provide a path to breach and steal South Korean classified military data, including wartime contingency plans jointly developed by South Korea and the United States.
- *NotPetya / MeDoc:* A tweaked version of MeDoc was infected with a backdoor to permit the delivery of a destructive payload disguised as ransomware. This attack paralyzed networks worldwide, shutting down or affecting operations of banks, companies, transportation and utilities. The cost of this attack to FedEx and Maersk was approximately $300 million each.
- *Kingslayer / Network Logs and Event-monitoring Tools:* Attackers targeted system administrator accounts to steal credentials in order to breach the system to replace the legitimate application and updates with a malware version containing an embedded backdoor. While it is unclear which and how many firms were ultimately infected, a United States defense contractor was, in fact, specifically targeted and compromised.

Attribution.

Attribution of these attacks has been undetermined, but technical and geographic aspects in many of the attacks point to hackers in Russia and China. That said, assigning culpability to Russian or Chinese intelligence services is both challenging and problematic. North Korea is developing as an actor in this attack space and likely made the bold and damaging attack against South Korea. It is suspected that:

- Russia developed and deployed NotPetya and Havex.
- China developed and deployed ShadowPad, XcodeGhost.
- North Korea developed and deployed the malware attack on the South Korean military.

Trust Is Broken.

Software supply chain attacks are particularly bothersome and insidious because they violate the basic and assumed trust between software provider and consumer. Customers have been correctly conditioned to buy and install software only from trusted sources and to download and use patches or updates only from authorized vendor sites. Now, customers must be wary of performing those basic, proper and prudent cybersecurity tasks when purchasing software and maintaining systems, since even authorized resources may be compromised.

Attackers have broken this trust by surreptitiously infecting software with malware in the development and distribution process in ways virtually impossible to detect. In these instances, attackers have successfully compromised the software development cycle and inserted malware before the code has been compiled and signed – therefore, creating a package that includes malware undetectable by typical customers and anti-virus, anti-malware programs. In other instances, attackers have disrupted distribution channels by placing dummy code, updates and patches on sites that customers use to obtain software releases and, ironically, security updates.

Note: Information contained in this paper represents the most reliable sources found in the public domain on the Internet for this topic. When available, documents were used from the Department of Homeland Security CERT; other recognized, authoritative, commercial sources (e.g., RSA, FireEye); and reputable, technology news outlets.