Teaching Case

JITTC

Journal of Information Technology Teaching Cases
1–6

DOI: 10.1177/2043886921993126
Journals.sagepub.com/jittc
SAGE

Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack

Pratim Datta[1,2]

Abstract

The connected world economy, compounded by the COVID-19 pandemic, has forced countries, companies, and organizations to pivot to digitally transforming their operations. Sophisticated, state-sponsored perpetrators have seized this forced pivot to lay the groundwork for Cyberwarfare with Advanced Persistent Threats. Using the 2020 Solarwinds Orion Sunburst hack campaign, this research uses a grounded case study approach to highlight the facets of the Sunburst cyberwarfare campaign. Findings suggest that cyberwarfare underscores the need for revisiting organizational processes, culture, and paradigms that are capitalized and leveraged by state-sponsored perpetrators. The Sunburst hack prompted organizations to immediately assume technical solutions. Among them, organizations were quick to isolate infected assets and patch infected systems. However, this research argues that such a reactive technical fix is a vicious trend based on a "wait, watch, react" ideology. Instead, there is prima facie need for process reengineering organizational operations and cultures to build and maintain preventive readiness.

Keywords

Process reengineering, cyberwarfare, Solarwinds, cyberattacks, Application Programming Interface, case study

Hannibal ad Portas

In 43 BC, Cicero, in his book of speeches, the *Philippics*, uttered *Hannibal at Portus* (Hannibal at the gates), invoking Hannibal's devastation of the formidable Roman army in the Italian peninsula in the battle of Cannae around 216 BC.

Cicero's phrase meant to imbue the Roman senate of an impending threat of having an enemy at the gates.

Hannibal's advance is not a story of brute force but that of process reengineering. Hannibal's campaigns relied on reengineering the traditional process of engaging the Roman army by choosing to traverse swamps and cross the Alps, and into Italy. Hannibal's 50,000 troops arrived in Cannae ahead of the 80,000 strong Roman force.

Instead of preparing traditional battle formations, Hannibal used his early arrival to control the supply chain. Hannibal's forces took control of the river, the only water source in the area. Hannibal positioned his troops north, forcing the parched Romans army to face the southern winds blowing dust into their faces. In short, Hannibal controlled the assets even before delivering a blow.

Forcing the Roman legions to march across a narrow corridor flanked by a deep river that he controlled, Hannibal subsequently enveloping the Roman legions and defeating them. The Romans, accustomed to traditional wide formations, were drawn into a trap, and defeated.

With a rapid proliferation of the Internet, IoTs (Internet of Things), and mobile devices, cyberwarfare is the new Hannibal—the new enemy at the gates.

Cyberwarfare

While cyberattacks are isolated incidents, cyberwarfare is a campaign. Cyberwarfare is a concerted and deliberate nation-state-sponsored cyberattacks, marked by continuous discovery of and capitalizing on digital and cyber-physical vulnerabilities aimed at adversely affecting a nation-state's economic and operational infrastructures.

[1]Kent State University, USA
[2]University of Johannesburg, South Africa

Corresponding author:
Pratim Datta, College of Business, Kent State University, Kent, OH 44242, USA.
Email: pdatta@kent.edu

Instead of amassing tanks, military personnel, and missiles by borders, cyberwarfare operators from any remote, global location, armed with a few computer programs, some savvy operators, and a network connection, can effectively disrupt another country's infrastructure and prompt chaos.

In popular culture, Q, the fictional head of MI6's R&D musingly remarks to James Bond, a fictional spy, "Well, I'll hazard I can do more damage on my laptop sitting in my pajamas before my first cup of Earl Grey than you can do in a year in the field" (Skyfall, 2012).

The function of cyberwarfare has also changed. The *raison d'etre* is no longer the assumption of physical territory but the practice of subterfuge, sabotage, and impairment that can hold a nation-state hostage without firing a single volley. It is the prolific Return on Investment of cyberwarfare that has attracted countries to build up their cyberwarfare arsenal, focusing on APTs (Advanced Persistent Threats)—sophisticated, continuous, destructive.

As the Sunburst hack will show, much like Hannibal's defeat of a more sophisticated Roman army in the battle of Cannae, a seemingly smaller state-actor can cripple a larger "global" foe by leveraging existing SOPs (Standard Operating Procedures) and reactive rather than proactive operational cultures of "don't fix it unless broken."

Digital meets physical: how hackers sabotaged Ukrainian artillery

Nearly every country with an active Internet infrastructure invests in both offensive and defensive cyberwarfare. During the 2014 Crimea operation, how GRU, Russia's espionage arm, is rumored to have collaborated with Fancy Bear (APT28), an infamous Russian hacker unit, to sabotage Ukrainian artillery sets the stage for the Sunburst.

As a part of the subterfuge, Fancy Bear used a combination of remote access command and control (C2) and Beacon malware to compromise Ukrainian artillery positions and destroy corresponding artillery (Volk, 2016).

Ukraine had an arsenal of 122 mm D-30 towed howitzers. Yaroslav Sherstuk, a Ukrainian artillery officer, had developed a program called "Попр-Д30.apk" (apk stands for Android Application Package meant for Android operating systems). The APK original Попр-Д30.apk could process targeting data faster and reduce the D-30 howitzer's targeting time from few minutes to 15 s.

Using Попр-Д30.apk as a template, Fancy Bear developed X-agent. X-agent was a malware implant that used a remote access C2 structure with RC4 cryptographic variant and a 50-base key. Fancy Bear distributed the malware APK variant via social media and military forums.

Between 2014 and 2016, the Ukrainian armed forces downloaded the malware Попр-Д30.apk. The APK carried a C2 Beacon, a malicious payload that would remotely communicate with the malware command and control from an infected Android device being used in the field. The malware infected devices remotely communicating to Fancy Bear's remote servers compromised the D-30 artillery locations, the battery strength, and movements, allowing Russian strikes on Ukrainian artillery, resulting in 20% D-30 howitzers lost in combat.

Fancy Bear's success with a remote access malware and a Beacon payload became a template that alleged state-sponsored actors that was followed in the Sunburst trojanized malware cyberhack.

The Sunburst [Solorigate] UNC2452 cyberattack

The Sunburst hack is a case-in-point of leveraging routine processes (Fireeye, 2020) in the software supply chain to adversely compromise multiple targets—a harbinger of the evolving nature of cyberwarfare.

The Sunburst cyberattack is not just a cyberattack but a cyberwarfare campaign. A cyberattack is an incident while cyberwarfare is operating on multiple fronts and over a sustained period of time. The Sunburst hack, instead of an overwhelming Denial of Service (DoS) shock-and-awe attack, capitalized on routine, suboptimal processes, to be passively pulled by Solarwind Orion client systems, remain dormant, sniff, and activate on proper target discovery, and then disguise and move laterally across the system. Please refer to the Appendix for a visual depiction of the Sunburst attack campaign sequence.

Choosing the attack vector

An attack vector is the mechanism by which cyber-threats find their way into a network or system. GitHub, a popular cloud-based software project repository used by companies to collaboratively develop software, automate workflows, has long served as a code warehouse. With so much activity and configurations in play, perpetrators behind the Sunburst hack may have found GitHub to be a fertile ground for capitalizing on a misconfigured code release. The perpetrators may have used the misconfigured public code release along with Solarwinds insecure update server credentials to inject malicious code into a component .dll and packaged it in a regular pull- or push-based patch update.

Moreover, the perpetrators realized serious misconfiguration and password vulnerabilities. In November 2019, Kumar, a cybersecurity researcher, warned that Solarwinds update server (where new software and security updates are posted) was accessible using a non-secure password "solarwinds123." It took Solarwinds 3 weeks to update the server password.

Increasing the attack surface

An attack surface is the amount and area that a cyber-threat can damage via an attack. Organizations need to reduce their attack surface to the minimal while cyber-threats seek to increase the attack surface to a maximum.

State-sponsored perpetrators identify Solarwinds Orion infrastructure monitoring software as a popular third-party cybersecurity and infrastructure monitoring software vendor to multiple organizations and industry verticals around the world, especially common across multiple US government agencies, including the Department of Defense.

In the Sunburst hack, the choice of the attack surface seemed predicated by two important assumptions. First, Solarwinds Orion infrastructure monitoring software had multiple client organizations, from government to companies, thus making Solarwinds a valuable common denominator for a hacking gateway into multiple organizations.

Second, Solarwinds Orion infrastructure monitoring and management software advised clients to exclude its software from anti-virus and EDR (End-Point Detection and Response) monitoring in order to reduce Type I errors (false positives from detecting routine activities as threats). This allowed for perpetrators to infiltrate the Orion gateway itself with the Sunburst hack, dramatically increasing the attack surface with multiple lines of access, communications, and control.

Building an attack infrastructure

Around, March–May 2020, the perpetrators set up an entire valid digital signature and encryption infrastructure to spoof authentication of their malware and make it look official, certified, and legitimate.

Using digital signatures, the perpetrators targeted computers running Microsoft Windows, creating multiple trojanized, Digitally Signed, innocuous-looking compressed components within the Windows Installer Patch files as a Solarwinds Orion software plug-in.

The plug-in update file contained a trojanized (hidden inside harmless-looking software like the Trojan Horse) malware compressed DLL (dynamic link library) component file called *SolarWinds.Orion.Core.BusinessLayer.dll*, is cleverly hidden within an "msp" (Microsoft patch), and is posted on the Solarwinds update website.

Reconnoitering the flanks

Several client organizations and industry verticals that regularly visited the Solarwinds update website unknowingly start installing the malicious DLL hiding within a legitimate *SolarWinds.BusinessLayerHost.exe* (a Microsoft Windows executable file).

The trojanized malware Sunburst remained dormant for 2 weeks and hid in plain sight to not raise any eyebrows from an out-of-the-ordinary "flaggable" surge in network traffic communications.

After a 2-week dormancy, the malware activated and started a multi-stage process.

Sunburst began by running a service in the background computer memory called Teardrop. Teardrop starts a new process thread (e.g. *netsetupsvc.dll*) utilizing a file called *gracious_truth.jpg* (masquerading as an image file). The Teardrop service deploys a malicious payload called Cobalt Strike's Beacon malware. Beacon uses popular HTTP, HTTPS, or DNS to hide as legitimate traffic while executing remote commands.

Sabotaging and evading

First, the malware uses a DGA (Domain Generation Algorithm) to establish a C2 server by resolving a subdomain of avsvmcloud [..].com, creating multiple fully qualified but malicious domain names such as xxx.appsync-api[.]eu-west-1[.]avsvmcloud[.]com.

This opened a communication backdoor!

With multiple malicious domains generated along with a common-and-control structure (think of a communication mothership), the DNS (domain name system) entries became a formal list of phonebook entries for safe communication—all set for remote access by the perpetrators!

With Machiavellian foresight, the perpetrators even mimicked legitimate hostnames on their C2 servers to avoid suspicion and detection and camouflage themselves.

To avoid detection, Sunburst operated like spies, moving laterally and constantly changing positions and credentials within the network. Sunburst also ensured that the credentials used for laterally moving within the network did not match the credentials used for remote access. Much like a spy that changes names, places, and codenames!

Sunburst started communicating with the malicious Command and Control domains.

Sunburst communicates as API (Application Programming Interface) communications. An API is an interface that links between multiple programs via certain protocols to share and translate information across many different types of software and architectures.

No cybersecurity flags were raised because Sunburst communications are cleverly disguised to mimic normal Solarwinds API communications from various Solarwinds clients to the enterprise.

Controlling and communicating

Sunburst ran a remotely controlled Job Execution Engine that can use the Beacon malware along with a network backdoor. Sunburst could now collect and communicate system and user profile information, change time, run malicious processes, terminate processes by their Process ID (PID), write to files, delete files, access the registry, and even reboot a system.

These actions are remotely communicating and controlled by a camouflaged backdoor using HTTP and mimicking normal activity as a part of OIP (Orion Improvement Program) protocol!

For a perpetrator, being able to control a process is tantamount to being able to stop essential processes from running, including backups, encryptions, and even audits!

Securing the gates

The Sunburst trojanized cyberattack exemplifies the growing sophistication in state-sponsored cyberattacks and the need to treat cybersecurity as an imperative with proactive process reengineering (Diffee and Datta, 2018).

Reengineer user processes

User (including vendor and consumer) errors are the weakest link, regardless of whether the user error is analog or automated (embedded in the operational logic): A Github misconfiguration error might have been the genesis for the Sunburst hack. Solarwinds server credentials that were supposed to be assigned as a private repository were instead released as a public repository, setting the stage for an attack.

Inadvertent misclassification and release of sensitive information have been a wellspring for malicious actors. In November 2017, users at Pentagon mistakenly released more than 100 GB of classified US Army and NSA (National Security Agency) data, called Red Disk, on a publicly accessible AWS (Amazon Web Services) server. The information included hashed passwords and private keys for access Pentagon resources (BBC, 2017). Fortuitously, a cybersecurity research group, UpGuard, discovered and reported the misplaced information back to the Pentagon and was peremptorily corrected, user errors, without a robust user process in place, can invite nefarious actors and actions.

Reengineer the software supply chain

Software has a supply chain. The software supply chain carries data packets and code from vendors to clients with the network as the logistics infrastructure. These data packets and codes originate from all across the world, hopping across nodes and warehouses around the globe. Some roads are safe; some are not. Some warehouses are legitimate; some are not. A packet can be hijacked, warehouses can be infiltrated, and malicious code can be injected into a legitimate-looking packet like a legitimate lorry hiding a terrorist.

The ability of the perpetrators to create a digital signature and certification infrastructure and implant and trojanize a Solarwinds Orion update underlines the need for revising authentication processes and protocols. The newfound cyberattack wisdom lies in evasion rather than the shock of awe of DoS attacks. APIs, which serve as logistics connectors across various software and systems in the global network, are particularly vulnerability in the software supply chain.

With an ever-spreading software supply chain, code integrity is critical. Therefore, ensuring the integrity of code repositories where vulnerabilities might be disclosed and malicious lookalikes could be injected.

Reengineer using a perpetrator's mindset

The Sunburst hack illustrates how sophisticated, encompassing hacks follow a philosophy of "invade and evade." These attacks rely on patiently waiting to scan the environment, choosing the most impactful target, attacking the target, and then disappearing into the woodwork by moving laterally across the network, acting like a legitimate source, and hiding in plain sight. The Sunburst malware hid in plain sight, embedding a malware payload inside a Solarwinds Orion update patch and relying on organizational routine patch downloads. Reengineering using a perpetrator's mindset reduces assumptions and obvious traditions. For example, Solarwinds Orion's recommendation to exclude itself from its clients' anti-virus and EDR monitors, that its clients omit Orion communications from its anti-virus, capitalized on a routinized, albeit, sub-optimal operational culture!

Perpetrators leverage organizations' long-held paradigmatic culture that cybersecurity is a black-and-white system. A black-and-white system is based on binary outcomes defined by discrete parameters. However, sophisticated cyberattacks are anything but discrete. Perpetrators in cyberwarfare understand and leverage, as the Sunburst hack reveals, these discrete cybersecurity parameters to infect and evade. Cybersecurity operational culture needs to rest on continuous interception and vetting of activities.

Reengineer based on defensive analytics

Data and pattern analysis are imperatives in understanding exceptions and suspicious behaviors from within applications and networks. There is a tendency, even a culture of focusing on zero-day exploits. The Sunburst burst was not a zero-day exploit but a passive, patient attack without raising suspicion. A zero-day exploit or a zero-day attack happens when perpetrators try to compromise software whose vulnerabilities have yet to be fixed or patched. Often, zero-day exploits focus on new software or system launches before all vulnerabilities are discovered and patched. Because zero-day exploits are much more anticipated, companies and organizations closely monitor any and all types of flaggable behaviors. However, over time, this readiness turns into complacence. Perpetrators behind the Sunburst hack capitalized on time and complacence, using the time to spoof a certification and authentication infrastructure and establishing a C2 center without raising suspicions.

Reengineer the network architecture

With more and more complex networks, compounded by the need to maintain operational continuity, organizations sacrifice their security for operational continuity and convenience. Such is the case during the COVID-19 crisis, where organizations hurriedly pivoted to digital transformation by allowing a variety of unknown BYOD (Bring Your Own Device) into the

corporate network. Managing such a dynamic and complicated meant reducing granular security and opting for a more generic set of security policies based on nebulous privileges, roles, and monitors—all based on trust and perimeter security—can become present vulnerabilities.

Trust-based network architectures often rely on perimeter fencing, great for collocated-secure corporate offices but confusingly complicated in more fluid, mobile work environments such as Work-From-Home (WFH). So, trust-based networks are simpler to manage but fall prey, as in the case of the Sunburst hack, to malware disguised as or embedded within a trusted entity.

Today, users might be logging in from a variety of secure and unsecure public networks using a variety of devices, some compromised and some secure. Therefore, managing devices and micro-transaction monitoring are central to building security in a fluid environment with malicious actors.

In contrast to trust-based networks, a *Zero-Trust network architecture* (e.g. Google's BeyondCorp initiative) forwards a granular device-level and transaction-level security based on device-specific credentialing, micro-segmentation and micro-privileges for all DAAS (Data, Assets, Application, Services). Zero-Trust network architectures need to infer and designate trust for every device, not based on historical transaction-level trust, device, and user credentials, but based on dynamic monitoring of managed devices, user credentials, and transactions. Transaction-level monitoring would have flagged Sunburst hack activities trying to create, communicate, and reconfigure any and all DAAS, offering faster response and quicker threat isolation.

Together, the Solarwinds Sunburst hack highlights the need for deliberate process reengineering across the entire software supply chain rather than building siloed fortifications. In an age marked by growing digital connectivity across critical economic and operational infrastructures, securing the borders is more than just a firewall fortification. Instead, cybersecurity operational mindset needs to shift from technical solutions to reengineering organizational processes and cultures to stay ahead of state-sponsored APTs.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Pratim Datta https://orcid.org/0000-0001-7371-4627

References

BBC (2017) Classified Pentagon data leaked on the public cloud. November. Available at: https://www.bbc.com/news/technology-42166004#:~:text=Classified%20Pentagon%20data%20was%20mistakenly,cyber%2Dsecurity%20researchers%20have%20discovered.&text=The%20hard%2-0drive%20had%20been,Security%20Command%2C%20in%20May%202013 (accessed 11 January 2021).

Diffee E and Datta P (2018) Cybersecurity: The three-headed Janus. *Journal of Information Technology Teaching Cases* *8*(2): 161–171.

Fireeye (2020) Highly evasive attacker leverages solarWinds supply chain to compromise multiple global victims with SUNBURST backdoor. 13 December. Available at: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html (accessed 11 January 2021).

Skyfall (2012) Directed by Sam Mendes. Produced by Barbara Broccoli.

Volk D (2016) Russian hackers tracked Ukrainian artillery units using Android implant: Report. *Reuters*, 22 December. Available at: https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU (accessed 11 January 2021).

Author biography

Pratim Datta is a professor of Digital Transformation and Cybersecurity at Kent State University and a senior research associate at the University of Johannesburg. Prior to academia, Pratim worked as a technology deployment and strategy consultant at global consulting firms. With nearly 50 journals publications in *JIT, CACM, EJIS, ISJ, JAIS*, and *CAIS*, Pratim researches socio-technical aspects of emerging technologies, information economics, digital transformation, and cybersecurity. Pratim also has multiple engineering inventions and actively works with the industry.

Appendix. The SUNBURST [SOLORIGATE] UNC2452 cyberattack campaign sequence.