Cybereason Intelligence Group

Owning the Battlefield

Fighting the Growing Trend of Destructive Cyber Attacks

Over the last two decades, there has been an increase in the quantity and specificity of destructive cyber attacks, especially attacks associated with nation state actors. Considering the level of destructive damage they caused, one would expect these attacks to involve sophisticated toolsets. However, in most of the cases we examined the attacks were carried out with relatively unsophisticated attack tools.

cybereason®

Apart from the Stuxnet and Crash Override/Industroyer attacks, most of the destructive malware utilized in the attacks reviewed in this report consist of basic techniques such as boot record wipers. These techniques are highly effective, yet relatively simple to code and execute. These trends would be alarming enough if they were not also coupled with an increase in “soft targeting.” The majority of the targets of known cyber attacks have been against civilians or private corporations (and the number of publicized attacks are a fraction of all attacks).

The attacks reviewed in this paper portray a clear picture: when nations leverage cyber attacks, the private sector ultimately pays the price.

Classifying a Specific Cyber Attack as Destructive

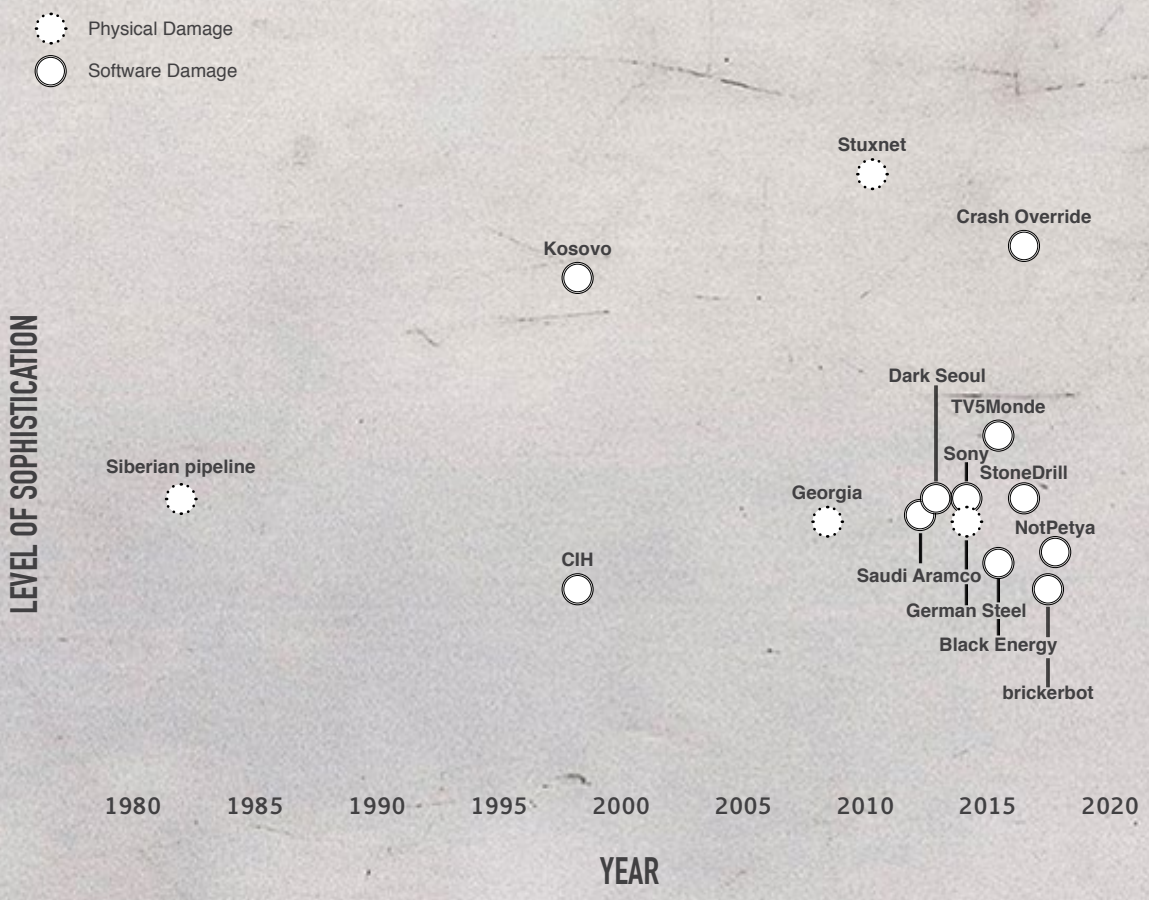
For the purposes of this paper, we’re using the definition of network attacks laid out in US DoD Joint Publication 3-13 where an instance of Computer Network Attack is “actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.”

We are intentionally excluding instances of Distributed Denial of Service (DDoS), website defacement, and ransomware attacks. While they arguably meet the Joint Pub definition, DDoS and defacement are often viewed as cyber vandalism. Their effect is orders of magnitude less severe than permanently destructive attacks. Ransomware, in our opinion, falls outside of the scope of this paper because their purpose is to force victims to pay the perpetrator, not deny or degrade a network. If a ransomware operation goes according to plan, victims will regain full access to their data. This is a radically different outcome compared to an operation with the goal of damaging a computer and network.

Growing Cadence, Limited Sophistication.

Our analysis of destructive cyber attacks from the 1980s to today shows a clear trend. Other than a small number of spectacularly sophisticated outliers, the general trend, especially since 2010, has been attacks that were carried out using relatively simple, but capable destructive malware. The most recent example, NotPetya, was composed of a basic destructive module that was paired with a fairly sophisticated and hard-to-detect backdoor. The destructive file was not overly sophisticated or did not contain novel capabilities.

Destructive Malware and Degree of Sophistication



As more actors become emboldened by the lack of consequences for conducting cyber attacks, we are going to see an increase in destructive cyber attacks. Most of them will be based on a “good enough” level of sophistication, capable of causing severe damage. Ultimately, cheap, dirty, and effective is all any actor needs to play in this arena, a realization that more actors are having, unfortunately. For the private sector this means an increased risk of being hit by unsophisticated, yet destructive attacks.

The Timeline of Destructive Cyber Attacks

1982\Siberian pipeline

In the early 1980s, the French government alerted the CIA that the Soviets had infiltrated a few U.S. laboratories, factories, and government agencies. This lead to one the most successful known counter-intelligence efforts in U.S. Cold War history.

The CIA learned about a "shopping list" of software that Moscow needed to operate a new natural gas pipeline in the western Ukraine. The CIA tricked the Soviet Union into acquiring software with built-in flaws. The software that ran the pipeline's pumps, turbines, and valves was programmed to malfunction after a certain interval, resulting in the pump's speeds being reset and valve settings producing pressure far beyond levels acceptable to pipeline joints and welds.

This resulted in one of the world's largest non-nuclear explosions. The explosion has been estimated at one-seventh the magnitude of the atomic bombs dropped on Japan during World War II. While there were no casualties, the attack completely vaporized part of the Soviet Union's Trans-Siberian Pipeline.

1998\CIH

CIH, also known as Chernobyl or Spacefiller, was a virus that overwrote critical system data. Approximately 60 million computers were believed to be infected by the virus internationally, resulting in an estimated $1 billion in commercial damages. Chen Ing-hau, who was a student at Tatung University in Taiwan, created the virus supposedly to counter the claims antivirus vendors made on the effectiveness of their software. Chen was not prosecuted since no victims came forward with a lawsuit. One of the impacted organizations included Boston College, which had a few hundred computer destroyed.

The media dubbed this virus "Chernobyl" because a few of its variants were programmed to activate on April 26 - the anniversary of the Chernobyl reactor meltdown.

CIH wiped data from hard drives and overwrote the BIOS chip, making the computer unusable. If CIH activated its payload, victim's machines required a hardware fix.

1998\Kosovo

During the Kosovo War, the U.S. military used cyber attacks in addition to bombing campaigns to reduce the effectiveness of Serbian air defense systems, which NATO concerned sophisticated and a threat to pilots. According to a U.S. government briefing paper on the campaign, the cyber attack had the potential to be a “great success” and involved using a computer network to strike the air defense system’s command and control center. However, the U.S. government has said that this briefing paper was an outline of a possible attack campaign and has not commented on the attack’s specific cyber attack components. However, the U.S. government did confirm that a group was formed to look into potential cyber attack scenarios.

2008\Georgia

Russian forces conducted a massive, joint arms campaign against Georgian targets in the summer of 2008. Some of the attack’s cyber operations included defacement of public and private websites, massive DDoS attacks, and diverting Georgia’s web traffic through Russia. Some of the impacted sites included the homepage of the Georgian president, the Ministries of Defense and Foreign Affairs as well as the sites of several Georgian media outlets and multiple private banks.

2010\Stuxnet

U.S. and Israeli cyber forces attacked the Iranian nuclear program in an attempt to slow down the country's ability to enrich uranium. Stuxnet, aka the world’s first digital weapon, was unlike any other virus or worm that came before. Instead of hijacking targeted computers or stealing information from them, it physically destroyed the centrifuges that enriched the uranium. Accomplishing this required intricate programming. Stuxnet had to target specific Siemens industrial control systems and CPUs. Additionally, the program had to determine that these systems were operating in Iran.

2012\Saudi Aramco

In a matter of hours, 35,000 computers at the Saudi Arabian government-owned oil company were partially wiped or totally destroyed and replaced with a picture of a burning American flag. The attack was attributed to Iranian actors that were retaliating against the Stuxnet attack.

2013\Dark Seoul

North Korean hackers attacked three South Korean television stations and two private banks with the DarkSeoul malware, which overwrote data and wiped infected drives. The attack, which impacted an estimated 32,000 computers, left many ATMs inoperable and customers were unable to make mobile payments.

2014\Sony Pictures Entertainment

In addition to causing significant data theft and subsequent data disclosure, North Korea's attack against Sony Pictures Entertainment also resulted in substantial damage to the company's IT infrastructure since the attackers used destructive hard drive tools to wipe the master boot record and erase all data. In an earnings call following the attack, Sony said that the hack would cost the entertainment studio $35 million. Most of that sum covered restoring Sony's financial and IT systems.

2014\German Steel Mill

Unknown attackers infected the Industrial Control System (ICS) of a German steel mill. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—but unspecified—damage. This is the second confirmed case in which a wholly cyber attack caused physical destruction of equipment. Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI). The attackers infiltrated the corporate network using a spear-phishing attack. Once the attackers got a foothold, they eventually compromised a "multitude" of systems, including industrial components on the production network. BSI did not name the company operating the plant nor when the attack actually took place. In addition, the report stated that the attackers and motivations were both unknown.

2015\TV5Monde

Russian actors used malware to destroy the hardware that controlled the TV station's operations. All 12 of the network's channels went off air for almost 12 hours. The actors broke into the network using multiple points of entry, including supplier networks such as the remote controlled cameras used in the studios. The attack cost the TV station $5.6m million and left it with an increased recurring bill of $3.4 million for improved security controls.

2015\Black Energy (Ukraine Power Grid)

Russian attackers, using a primarily open source toolkit, managed to attack three Ukrainian energy distribution companies and cut power to approximately 225,000 customers. Public reports indicate that the Black Energy malware was discovered on the companies' computer networks. (The role of Black Energy in this event remains unknown pending further technical analysis.)

2016\StoneDrill

Iranian hackers leveraged drive wiping tools to attack Saudi Arabian targets in government, private sector, telecommunication, and transportation. By infiltrating the browser instead of drives, StoneDrill is more likely to remain undetected for the time it needs to wipe data. It does this by overwriting both physical and logical drives with random numbers -- rendering drives useless and making information impossible to recover.

2016\Crash Override

Hackers used this malware to strike an electric transmission station north of the city of Kiev, blacking out a portion of the Ukrainian capital (equivalent to a fifth of its total power capacity). The malware was designed to attack ICS systems associated with power grids. The malware was built to delete data and disrupt IT systems as well as physically damage ICS systems. According to US-CERT, there is currently "no evidence to suggest this malware has affected U.S. critical infrastructure. However, the tactics, techniques, and procedures (TTPs) described as part of the Crash Override malware could be modified to target U.S. critical information networks and systems."

2017\brickerbot

This simple piece of malware attacks insecure IoT devices and formats their internal memory, rendering the device useless. The author nicknamed, janit0r, has claimed to have bricked upwards of 2 million devices. The destructive actions caught the attention of ICS-CERT and they issued alerts (in April) warning organizations to disable Telnet and SSH access to their devices and asked owners to change the device's default factory setting passwords.

2017\NotPetya

This self-propagating malware infected approximately 25,000 computers with the aim of wiping their hard drives when the machines rebooted. The majority of the victims were in the Ukraine. However, at least a dozen large multi-national companies were also impacted, including shipping company Maersk, advertising group WPP, and the consumer goods company Reckitt Benckiser, which reported that annual sales would increase by 2 percent instead of three percent. The company did not provide financial details, but based on last year's sales figures, a 1 percent cut to the full-year forecast would be worth about £100 million pounds ($130 million).

Even though the majority of cyber incidents are still motivated by espionage or criminal activity, the increased use of destructive tools, especially by nation-state actors, is an alarming and growing trend. The private sector can't dismiss the security repercussions of this development.

Great Gain, Little Consequence.

Destructive attacks serve a variety of purposes for nation states: they can signal displeasure, retaliate for another's actions, or conduct disruptive covert operations with impunity. The relative ease of striking internationally combined with the comparative lack of retribution has created an environment where nations will continue to experiment and grow increasingly bold in their attacks. At the end of the day there is no reason for nations to stop this behavior.

Despite pronouncements such as NATO's ability to invoke Article 5 based on a cyber attack and the countless discussions of deterrence in cyber space, we currently reside in a cyber environment that appears far more nasty and brutish than the noble system that was meant to usher in an age of stability.

Governments are currently reticent to engage in retaliation and any action that may escalate cyber attacks from actions taken in the digital world to actions taken in the physical world since the cost for retribution in this domain is significantly higher. An out of domain relation, especially from the military, results in an escalation ladder that neither the victim nor the attacker's government understands or can control.

This fear of uncontrolled escalation means that governments are unable and unwilling to effectively cordon off sectors of the Internet from this type of attack. Because of this policy paralysis, coupled with a compelling and often more articulated stated case from the offensive components within government, it is unlikely that we will see a large policy shift driven by the governments with the largest offensive and defensive capabilities.

Indeed, the immaturity with which cyber deterrence has been wielded so far suggests that states fail to take cyber seriously and do not see it as a domain in which their actions will bear consequences. The idea that a major power would threaten the critical infrastructure of another major power over an information operation would be preposterous if the threat was carried out via physical means. The threat also served as a green light to any state that would like to hack critical infrastructure, because now it is for "deterrence" rather than offensive effect.

Governments are still in the process of understanding cyber space, escalation, and the real world effects of cyber attacks. But they are still rushing to use these capabilities because they can provide significant means to strike across great distances and against targets traditionally considered escalatory and war inciting.

With no ability, or even intent to dissuade destructive attacks from nation states, the private sector is paying the ultimate price. They are most often the victims of these attacks because they are both less secure than government networks and also have been largely deemed a "safe" target from a retaliation standpoint.

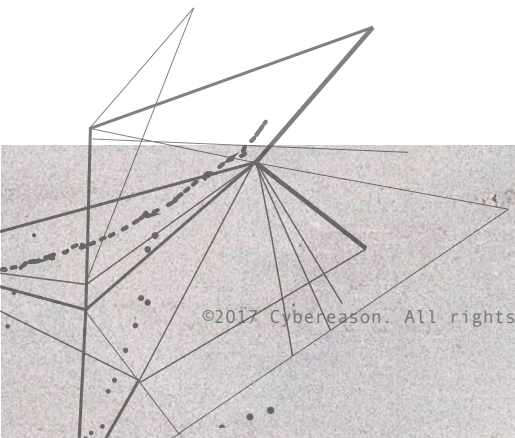
What Happens if Our Current Trajectory Goes Unchecked?

Absent any consequences for the attacker, nations will continue to experiment with cyber-attack capabilities and hone their ability to use them for multiple purposes. This means that the cluster of attacks with a relatively low sophistication level will likely to continue grow year over year. The victims will likely continue to be non-government institutions that for some reason present a useful target for advancing a hostile nation's interests.

An even more worrying development is the adoption of these tactics by non-state actors. Currently, DDoS is the easiest and most leveraged tool for hacktivists and those looking to disrupt specific entities. However, as more destructive tools continue to be used and society continues to become numb to reports of new attacks, cyber criminals and hacktivists will increasingly move into this space. The ability to have a larger, more lasting impact combined with the ability to increase obfuscation by not only damaging information systems but also wiping forensic evidence will become ever more enticing for those who want to expand their business model. Accelerating this trend will be the continued and seemingly increasing nature of leaked advanced tools and capabilities.

Avoiding Inertia

If we cannot rely on governments to put their shiny new toys back in the box for the sake of Internet security and we can expect an increase in attacks from non-state actors without a commiserate increase in arrests and prosecutions of the perpetrators, what is the private sector left with beyond a short and brutal life?



Recently, a couple of ideas have been discussed to help handle this situation. However, they may end up creating a more difficult environment for all:

- **Deterrence by denial** has been a phrase thrown around a lot lately. To achieve this, cyber security must evolve to a point where companies can afford stalemate inducing defensive technologies.
- **Hacking back** is another concept that is rearing its head again. There is even a bill in the U.S. House of Representatives that would allow the use of this type of behavior even if within limited boundaries. However, this type of deputizing of the private sector is only going to lead to more hacking, less secure networks, and in general a shorter and more brutal life for corporation's network security.

Unfortunately, technology, treaties, and self-restraint will not interrupt this growing threat. An adversary with significant motivation, resources, and time will be able to crack any combination of technology put in place to passively interrupt them.

The Response Plan: Know When War is Declared, then Own the Battlefield

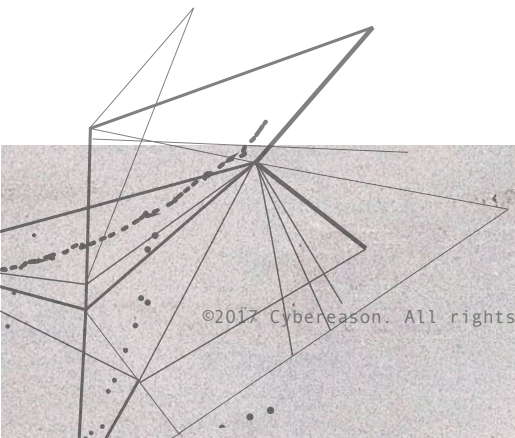
Actionable information is the best weapon

For the private sector, the best near term hope to withstand this period of instability and increased hostility is actionable information. Destructive attacks are a small subset of the overall threats organizations are facing. The motivations for carrying out these attacks and the access and capabilities required to effectively conduct them allow the development of a relatively accurate modeling of what is likely to cause a private entity to become a victim of destructive attack. This can help organizations realize how to minimize the probability of an attack's success. Understanding why a company is an appealing target for a nation state lashing out allows it to apply more effective counter measures.

Use time to your advantage

Thankfully, time can work in the private sector's advantage. The moment the actor initiates contact with a network in the private sector - the race against the clock starts. Can the threat actor achieve their goal of causing destruction of the networks and information, before they are detected and diverted to spending their time attempting to maintain access rather than achieving their objective? Right now, this race condition largely exists in theory. The time from breach to discovery is measured in weeks if not months for most networks. This is far too long to stop these types of destructive attacks. Only through the use of intelligence, hunting, and active monitoring can the private sector reduce victimization.

These strategies must be tested and perfected now. While the current rate of large-scale cyber attacks is small in comparison to the rest of the threats facing corporate networks, their disproportionate costs, and the trend of increasing frequency means our window for experimenting with and building effective defenses is closing. The current opportunity to disrupt the efficacy of these operations has the potential to divert the current trends of using cyber as an easy, inconsequential way to lash out in the international system.



About Cybereason Intelligence Group

The Cybereason Intelligence Group was formed with the unique mission of providing context to the most sophisticated threat actors. The group's members include experts in cyber security and international security from various government agencies, including the Israel Defense Forces' Unit 8200, which is dedicated to conducting offensive cyber operations. Their primary purpose is to examine and explain the Who and the Why behind cyber attacks, so that companies and individuals can better protect themselves..

Cybereason is the leading provider of behavioral-based enterprise attack protection, including endpoint detection and response (EDR), next-generation antivirus (NGAV), and active monitoring services. The Cybereason solution reduces security risk, provides complete visibility, and increases analyst efficiency and effectiveness. Cybereason partners with enterprises to gain the upper hand over adversaries.