WHITE PAPER

SentinelOne
The future of endpoint security

The Democratization of Nation-State Attacks

Introduction

Cyber-espionage is not new.
The first documented hack of U.S. systems by a foreign power was in 1986, when Marcus Hess, a German citizen, hacked ARPANET (Advanced Research Project Agency Network) subsequently attacking industrial controllers. Additionally, Hess began selling pilfered information to the KGB. He was caught when a security researcher recognized a seventy-five cent accounting error in his university's network. Over the next three decades, the world's intelligence agencies played an escalating game of cat and mouse via the Internet.

> In 2010, the game changed. This year was heralded by the arrival of Stuxnet, the malware that arguably escalated the game of cyber-intelligence into true cyber-warfare.

Stuxnet was able to destroy centrifuges at the Iranian nuclear refinement facility in Natanz. Nothing like Stuxnet had ever been seen before—a weapon made entirely of code, one that was able to damage targets in the real world.

Stuxnet required a massive amount of effort. Two successive presidential administrations worked on its particulars, which required the cooperation of two intelligence agencies, and the building of a real-world test site. All of its components were built from the ground-up. In a way, Stuxnet's complexity was reassuring. It meant that any other government willing to try out an attack of a similar scale would have to go to similar lengths. In 2015, however, the game changed again.

In the winter of that year, hackers— apparently directed by the Russian government—were able to crash the Ukrainian electrical grid using malware known as Blackenergy. This malware was completely unlike Stuxnet. It was built from mostly off-the-shelf components, targeted at a run-of-the mill utility rather than a specialized research project, and presumably required no specialized engineering knowledge to execute. What's more, the Stuxnet hack was aimed at government-sponsored research in a government installation. The Blackenergy attack was targeted at civilians. These differences are worrying.

Twenty-four years elapsed between the first documented case of cyber-espionage, and the first outbreak of cyber-war. Only five years elapsed between the first successful cyberwarfare attack and the second. Security professionals should be concerned that this is a sign of things to come. Should we prepare for a future where cyberwarfare attacks, directed at physical infrastructure, become more frequent, more successful, and aimed at civilian targets?

Stuxnet and Operation Olympic Games

Prompted by fears of an Iranian nuclear program, President George W. Bush inaugurated Operation Olympic Games, the research program that would eventually give rise to Stuxnet. According to a German industrial expert, Ralph Langner, Stuxnet could be likened to, "the arrival of an F-35 fighter jet on a World War I battlefield."

> In truth, Stuxnet was more of a smart bomb—a JDAM, not a Joint Strike Fighter. That's because Stuxnet was designed to affect only a single hardened target.

The planners at Iran's nuclear refinement facility in Natanz may have known that they would eventually come under cyberattack. Initial mapping of the Natanz facility was conducted with malware known as "beacon code." When the time came to map the more sensitive areas of the Natanz facility, this code was deflected by one of the most effective counter-measures ever deployed against malware—an air gap.

Air gapped computers have inherently powerful defenses against malware. With no wired or wireless connections to the internet, there are only a few ways to infect them. Researchers at Ben Gurion University have discovered ways to attack air gapped systems using fan noises, heat, inexpensive cellphones, and more, but as of 2008, when the Stuxnet hack was first carried out, the only way to hack an air gapped system was via an infected USB drive. Considering the unlikelihood of a Stuxnet-infected USB drive making its way into an Iranian nuclear enrichment facility by accident, it's likely that the initial infection was accomplished by one or more malicious insiders, possibly supplied by the Israeli intelligence agency, Mossad.

Once implanted into the Natanz intranet, Stuxnet began scanning infected endpoints for Siemens ICS software. Once this software was discovered by the malware, Stuxnet would root the ICS, and then send signals which would make the connected centrifuges behave erratically, shaking themselves apart. At the same time, they would spoof the control sensors so that automatic fail-safes would not activate upon detecting abnormal behavior.

Unintended Consequences

The first unintended consequence of the Stuxnet malware was its detection. With any malware attack, a primary objective is to accomplish one's goal without anyone knowing that anything happened. For Stuxnet, which represented an attack on a sovereign nation that the United States was not at war with, that certainly was important. Stuxnet was supposed to delete itself whenever it found an endpoint without any Siemens ICS software on it, and this mechanism was supposed to prevent it from escaping the confines of the nuclear facility. Nonetheless, Stuxnet did escape, and began to replicate in the wild.

Leaving aside, for the moment, the political ramifications of Stuxnet's discovery, the results of its attack were mixed. While Stuxnet did in fact achieve its stated mission of damaging Iranian centrifuges—1000 out of 5000 total devices were destroyed—it's debatable as to whether this actually had a lasting impact. Economic sanctions and treaty negotiations incentivized the Iranian government to begin stepping down their nuclear program shortly thereafter.

> What Stuxnet really highlights is the sheer complexity, at least in 2008 terms, of creating a cyberattack that can damage industrial assets in the real world.

To recap, Stuxnet involved at least four years of work, the efforts of two successive US presidential administrations, and collaborations between the US and Israeli intelligence agencies that involved several on the ground personnel. Additionally, once it was determined that the Natanz facility was using centrifuges of a model once used by Muammar Gaddafi, the US actually took the additional step of using centrifuges seized from Libya in order to construct a physical replica of the Natanz plant.

> Creating a cyberattack that successfully targets physical infrastructure is difficult. It is beyond the reach of almost anyone except an extremely well resourced government institution.

Creating a cyberattack targeting physical infrastructure requires planning, expert knowledge of physical systems, on-the-ground assets, time, and money. As a counterexample, witness the case of an Iranian Revolutionary Guard hacker who breached the ICS controls on the Bowman Avenue dam in upstate New York. This attack, which was attempted in 2013, involved only time and effort, and didn't involve the coordination of any on-the-ground assets. As a result, the hacker a.) didn't realize that the ICS controls that he breached were down for maintenance at the time rendering them useless, and b.) was about the size of a garage door. Were it tampered with, it would have flooded exactly one neighborhood's worth of basements. It was not a history-making breach, by any means.

With all that being said, Russia's Blackenergy attack on Ukraine proves that for governments who do have the resources, launching cyberattacks against physical infrastructure has become less and less of a challenge.

Blackenergy: An Alarming Evolution

On December 23rd, 2015, large areas of Ukraine lost power due to what was later confirmed to be a sophisticated malware attack. Power plant operators at the Prykarpattyaoblenergo control center got the shock of their lives as they watched remote users take control of their machines' cursors, lock them out, and then proceed to open the breakers and cut off power to thousands of Ukrainian citizens. As a coup de grâce, the attackers used a KillDisk subroutine to overwrite the firmware on the SCADA controllers that operated several electrical substations—relegating them to manual operation for several months

The primary mechanism that allowed the attackers (and for the purposes of this document, one will assume that the attackers were Russian) access to the Ukrainian control center was a piece of malware known as Blackenergy..

This malicious software, Blackenergy, was hidden in a Microsoft Word document as part of a phishing attempt that encouraged workers to enable macros in order to view a file.

Once enabled, Blackenergy infected their endpoints, and hid.

The hackers used Blackenergy to map the utility's corporate network slowly, over a matter of months. Eventually, they discovered the user credentials that allowed workers to access the SCADA network that controlled the breakers at their various substations. Since the workers were not required to use two-factor authentication to log into the SCADA network, it became child's play for them to log in an accomplish the first successful act of cyber-war since Stuxnet itself.

The similarities between the Blackenergy attack and Stuxnet are more alarming than their differences. As with the Stuxnet attacks, they used prototype versions of their malware to find targets for an attack against ICS devices. Where US and Israel only scouted a single facility, however, Blackenergy prototypes have been found all over Europe for years prior to the 2015 attack. In fact, prior to the Ukraine hack, Blackenergy was thought to be merely a commonplace tool for industrial espionage. Now it looks as though Russia may be able to tamper with industrial devices all over Europe, practically at their whim.

Secondly, while Stuxnet broke new ground in terms of its capabilities, the weaponized variant of Blackenergy is essentially built of COTS (commercial off-the-shelf) components. The individual modules of Blackenergy have been available on various darknets for years. Essentially, any hacker with the sufficient skill can now put together malware that's essentially identical to the malware used in the attack on Ukraine's energy grid. Although such attacks may have a lesser chance of success because they're not backed by nation-state resources, all it takes is one successful attack for a nuisance to escalate into a crisis.

Similarities and Ramifications

It is a bit clichéd to suggest that a single event might uncork a can of worms that leads inevitably to disaster, but as far as the Stuxnet attack is concerned, there are real reasons to believe that it may have kicked off a trend. The successive iterations of Blackenergy suggest that Russia has a serious interest in not only refining the tools of cyberwarfare, but also making those tools accessible to a common variety of criminals.

This pattern of behavior is quite typical of Russian espionage, counterintelligence, and propaganda campaigns. Rather than directly advocate their policies, they tend to prefer to outsource their foreign and social policy platform via a massive "troll army," dedicated to publishing pro-Russia commentary on the internet and social media. By demonstrating how easy it is to hack nation-state opponents with publically available tools, Russia is now arming its supporters with the tools of cyber-war.

If this goes on, the industry could experience no shortage of negative outcomes. Ransomware attacks that paralyzed hospitals made headlines in 2016. Imagine the fever pitch of hysteria of America's light, heat, and water were similarly held for ransom?

Once enabled, Blackenergy infected their endpoints, and hid.

The information security industry should not count on the fact that attacks on infrastructure have historically been confined to state-level actors. The Stuxnet attack may as well have been a blueprint for other states to launch attacks on their own. The Blackenergy attack, with its reliance on consumer-grade malware, may as well have been a blueprint for scammers and hacktivists.

In short, the directors of utilities and other public infrastructure companies must immediately consider how to best protect themselves against advanced malware.

What Does Axiomatic Security Look Like in the Data Center?

Utilities, factories, and other entities that rely heavily on capital equipment must invest in a solution that can detect and mitigate unprecedented attacks. Stuxnet and Blackenergy both used components that haven't been seen before in the wild, and while signatures for them have been written, it's almost a guarantee that similarly novel malware will be used in the next attack.

SentinelOne offers a next generation endpoint protection platform that is effective against attacks both known and unknown. Crucially, this solution offers the ability not just to stop threats, but also undo the damage they have caused—essential in a case where attackers may have overwritten the firmware on vital machinery.

As stated, only five years passed between the first known nation-state attack on infrastructure and the second. It would be a mistake to assume that five years will pass before the next attack. The time for utilities to fortify their infrastructure is now.

SentinelOne
The future of endpoint security

For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com