Squirrels - Knowing Your Real Threats

By Bianca Capretta

May 7th, 2018

Abstract

In Washington DC, the government has been long warned about the threat of "cyberwar" against critical infrastructure. Hackers could bring down power grids, financial institutions, and other important systems for our world. However, the damage done so far by hackers has been small or exaggerated. What people do not realize is that the real problem is stemming from small, fuzzy-tailed creatures - *squirrels*. Chewing through the insulated power lines or burrowing their way into substations, they can strike at any moment and leave thousands of people instantly powerless.

Some news focuses on inconsequential cyber threats (like malware that uses sound to jump air gaps to infect other computers) but in actuality, little is happening there. What people don't realize is that squirrels are winning the cyber war. The number of animal-induced infrastructure outages far outweighs the number of real cyber attacks worldwide (Gallagher, 2017). As of 2018, a website called CyberSquirrel1.com has collected the total number of successful cyber war ops, and it came out to 1,141 attacks from squirrels alone and only three attacks from humans. Other animals are also helping squirrels in this endeavor - such as birds, snakes, raccoons, rats, beavers, and even jellyfish. This paper aims to analyze news coverage of cyber attacks made by both humans and squirrels to see who is truly wining the cyberwar.

1 Introduction

A ripped hole in the window screen and dispersed jagged avocado peels throughout the kitchen were the first pieces of evidence. My roommate Rachel messaged me about a mysterious break-in and the sad reality of my stolen avocado. We realized a squirrel had bitten through the screen parallel to our open window, aggressively ate my precious avocado, and ran away leaving an obvious trace of attack. Even with a coincidental security company named Sqrrl, nothing stopped this actual squirrel from breaking into and entering my home. While a silly and minuscule plot at the end of the day, we cannot dismiss the power of the squirrel.

How much impact can squirrels really have beyond taking one's food? Well, so much that there is now a coined term after them: squirrel power. In Tampa, Florida in 2013, a squirrel cut electricity to 700 people by electrocuting itself on a power line, which led to a delay across three different schools' statewide achievement tests nearby. Thousands of people were naturally frustrated by this squirrel power as it disrupted their electrified lives for hours (Mooallem, 2013). A man named Cris Thomas created a website called **CyberSquirrel1** that has been documenting Cyber Squirrel Operations like that since 1987 where squirrels, and even other animals, take out city lights.

Some people think it is all just a funny joke. "Squirrels are staging an uprising" or "squirrels are calculating, nut-cheeked saboteurs trying to overthrow humanity" (Mooallem,

2013). But in reality, squirrels spend their entire lives teething, chewing through wires (Bartels, 2016). When news covers big hacks, it is hard for people not to believe the hype on media; however, most reported hacks to critical infrastructure are not even cyber-related. For example, a hacker was blamed for the Turkey BTC pipeline explosion in 2008; however, a local rebel group actually just used conventional explosives, not connected to the internet. Since 1987, only three recorded human hackers have brought down city power, while a whopping 1,141 number of squirrels have achieved the same.

When it comes to attacking the power grid, our worries should not be directed at human hackers, but at squirrels. As the past deputy director of NSA John C. Inglis phrased it, "I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels" (cybersquirrel1.com). For the past 35 years of the cyberwar, security at most power companies has not been paying attention to their real threats. According to some security experts, the risk of squirrels damaging the electrical grid is more serious than the risk of cyberattacks.

1.1 Why I Chose This Topic

It is almost comical how much squirrels have been underestimated. With 560 power outages in Montana in 2015 alone, they are not just winning, but *crushing* the cyberwar. Most government and industry officials can't see how much damage is really being done by animals, so this paper is an attempt at counteracting the crazy claims made by "cyberwar hawks" and the inaccurate conversations surrounding supposed alleged human hacks on the power grid. People are spewing facts they do not know so the current information afloat needs to be discussed.

The shocking statistics start with CyberSquirrel1.com. The website began as a hobby, but has actually tracked the most data on squirrels and other animals taking down infrastructure. The DoE Office of Electricity Delivery and Energy Reliability, on the other hand, has collected no helpful statistics about animals; they only track outages that impact 50,000 people or more that last for at least 60 minutes. By only considering large-scale electrical outages, they have been ignoring the increasingly large accumulation of small attacks made by animals, which could have shed some important light on what is truly harming critical infrastructure in the US.

CyberSquirrel1 has kept track of over 1,700 animal-caused power outages affecting nearly 5 million people for over 30 years. If one consolidated this amount of energy into a single location, it would essentially take out power in the San Francisco Metropolitan area for two months (Gallagher, 2017). The current hype targets the high possibility of risk from human cyber attacks; however, current precautions in protecting our infrastructure from animals like squirrels, raccoons, or even snakes has failed. Handling the cyberwar is not just about securing software, but about improving our physical infrastructure to prevent, or at least reduce, animal attacks from happening again. Squirrels taking down our lights is not just a satire; we need to put the threats of cyberwar into perspective.

2 Cyber/Technology Attacks

2.1 Squirrels Ruining Infrastructure

Why has physical infrastructure proven to be so weak when exposed to these small bushy-tailed creatures? Let's first take a look at what happens when a squirrel happens upon a power line. According to the Electric Power Research Institute, a squirrel typically creates a blackout by scurrying across electrical equipment, simultaneously touching both an energized section and a grounded piece of equipment (Mooallem, 2013). When a squirrel generates this arc finishing the circuit, a flash of blue light immediately ignites, killing the squirrel at the center.

Grids, however, are actually designed to deal with this violent incident. When a dead animal falls to the ground, ending the interference, the electrical flow should continue as normal. But if the squirrel carcass stays put and does not fall to the ground, the body can trigger a "continuous fault" which stops the revived electrical flow, again (Mooallem, 2013). When the electrical grid cannot find a way around the dead squirrel's body, the lights go out. Circuit breakers that burn out or costly equipment that becomes ruined can be expensive to clean and replace.

2.2 Cyber Attacks Caused By Humans

Do not be fooled. Human hackers have been falsely accredited for creating blackouts when they didn't even create the problem in the first place. For example, close to 50 power outages in Brazil from 2005 to 2007 were erroneously blamed on cyberattacks, when in reality sooty insulators were the source of the outages. Everyone believed it was the work of hackers, though; even "60 Minutes" repeated the claim on live television (Soares, 2009). Another example includes a Baku-Tbilisi-Ceyhan (BTC) pipeline explosion in Turkey. Even though the owner of the pipeline mentioned that a faucet in the explosion was not connected to the main grid network, four separate sources claimed that the explosion's source came from a cyberattack (Tanriverdi, 2015).

In 2011, news revealed that "Russians Hacked [a] Water Plant" in Illinois; however, no evidence could be found to confirm that a hacker had performed the destruction (Zetter, 2011). A Russian IP address had been incorrectly linked to the failure by a government intelligence center. Months earlier, the man in charge of the utility control system had actually been on vacation in Russia remotely accessing data on the water facility. Incorrectly connecting the water pump failure to a Russian hacker could have been proven otherwise with one phone call.

The Bowman Avenue Dam controlling water on the Blind Brook near Rye, New York broke in 2013; however, the city manager released news that Iranian hackers performed the damage (MyRye, 2015). Since Iranian hackers had control of a nearby small dam two years prior, concerned officials at the White House pointed their fingers at Iranian hackers again. A sluice gate was originally built to control water flow during storm events; controlled to open and close by a computer, it was the only electronically controlled item in the dam (MyRye, 2015). The Department of Homeland Security investigated the "attack" while the gate wasn't operating

correctly, though, and they confirmed it was never operated by any unauthorized people outside of the city.

Like the boy who cried wolf, all these stories led cybersecurity pros to not believe in hackers so easily; however, there are a couple instances to fear the human hacker. Around Christmas time in 2015, a regional power company blamed the numerous power outages in Ukraine on malware for turning off the substations (Rogue, 2016). Cyber-hawks approached this claim of blame with skepticism; however, a real sample of malware was found which people considered to be strong evidence. There still remains disagreement, though, whether the malware in the company's system came from cybercriminals, work from a nation state, or an infection that could have spurred randomly in the system.

The only fully confirmed infrastructure cyberattack resulting in real physical damage is known as Stuxnet. Stuxnet is an intricate and complicated computer worm that mainly exploits software vulnerabilities in power plants focused on uranium enrichment (Fruhlinger, 2017). The worm takes over the programmable logic controllers (PLCs), spinning the centrifuges faster and longer than they should be, in turn ruining the delicate equipment; meanwhile, the monitors can't detect any problem in the system so the problem keeps growing. With development for Stuxnet beginning around 2005, it was a joint operational effort by US and Israel to stable Iran's Uranian enrichment centrifuges (Fruhlinger, 2017).

Despite all the hype and fear of human hackers, squirrels and other animals have produced countless power outages across the world. The biggest threat to the US power grid is not human, but rather a small creature that likes acorns.

2.4 Cyber/Technology Attacks Caused By Animals

Did you know there has been a power outage by an animal in every state in the US (even a chicken in Hawaii)? With such a large attack surface for animals, from power lines to stormwater treatments across the country, reconnaissance has been conducted to gather data regarding the damage conducted by animals. In 1987, a squirrel shut down the NASDAQ for over an hour, halting the trade of around 20 million shares (Peterson, 2016). A pain in the neck for firms across the country, squirrels have been a nuisance for more people than one would expect.

There actually exists an acronym P.O.C.B.S. (power outages caused by squirrels) to refer to these unfortunately frequent events. Squirrels have caused blackouts in a Trader Joe's in South Carolina, a university in Montana, a Veterans Affairs hospital in Tennessee, and an airport in Virginia (Mooallem, 2013). Under a week after the Trader Joe's incident, 7,200 people lost power to another squirrel in Rock Hill, South Carolina. The city officials claimed that squirrel attacks were quite rare and that their grid was "still a reliable system"; however, 3,800 more people lost power nine days later when a squirrel caused the explosion of a circuit breaker in a nearby town (Mooallem, 2013).

Out west in Portland, Oregon, squirrels brought down a total of 19,740 people's lights in under a month on three separate occasions. Over 10,000 people in Kentucky encountered two P.O.C.B.S. within a week. At the Academy of Fine Arts in Lynchburg, Virginia, people used their iPhone flashlights to view the art because two huge P.O.C.B.S. a week apart left the building dark (Moollaem, 2013). Under a month later, a squirrel caused another blackout in Kalamazoo, Michigan for 2,000 people, and then again to around 1,000 people a week later.

The number and examples of P.O.C.B.S. could go on, but squirrels are not the only culprit. Other animals like birds, raccoons, and sharks have also shown to take out infrastructure and more. In 2016, a vervet monkey caused a four hour blackout in most of Kenya by infiltrating a power plant; the monkey slipped off the roof and fell onto a transformer which caused a chain of transformers to fail. A beech marten (a small rodent) did not survive when it put the Large Hadron Collider out of commission for a few days by shorting out its power supply (Bartels, 2016).

Squirrels are not the only animals chewing cables. Sharks were once found biting into transoceanic fiberoptic cables. They likely were attracted by the cables' electromagnetic fields (Bartels, 2016). Some raccoons attacked a particle accelerator called Tevatron, taking down the company for a few days. Despite airport attempts made to keep birds away, many gulls have collided with airplanes, costing millions of dollars a year (Bartels, 2016). And once a jellyfish clogged the pipes of a nuclear reactor.

2.4 Defenses

Utility companies have actually been attempting to fix these problems by adding numerous wildlife deterrents on top of their equipment. Tools like "arrester caps" and "bushing covers" make squirrels lose their balance (Mooallem, 2013). Companies have also tried other methods to discourage squirrels from crawling on power lines, such as spraying areas with fox urine and coloring equipment with red paint; however, these attempts have both failed as squirrels might not even able to process the color red (Mooallem, 2013). Some companies have placed plastic owls on building exteriors to prevent pigeons from landing on them; however, a substation outage once occurred when a hawk attacked a fake owl.

As one can see, the current attempts at preventing squirrel-related infrastructure attacks have not been the most successful. Given that squirrels have had such a large impact on the US electrical grid, more time and energy should be spent on making better squirrel guards and various gadgets to prevent animals from running or landing on power lines. For example, a tame yet shocking taser for animals could be built on top of power lines to keep animals away from harming actual infrastructure. A "bug spray" for squirrels could also be chemically concocted to keep them off power lines.

Again, the problem lies beyond squirrels. For example, jellyfish have clogged the pipes of a Swedish nuclear reactor, forcing a plant shutdown (The Guardian, 2013). Water pipes can be improved with a more secure under-water fence so that jellyfish can't be so easily washed into the metal workings of the machinery. The Institute of Electrical and Electronics Engineers

(IEEE) has the power to make our critical infrastructure stronger and better, and should start to take the initiative to do so.

3 Conclusion

Do not be a fool wasting your time on cyber hacks and blaming humans for the damage; animals are doing more of it than we think. If industry security sectors began to notice that the real problem lies with animals, they could rearrange their priorities and think about their defenses more appropriately. Stuxnet serves as a prime example of human-built malware bringing down critical infrastructure, but no other human-inducing cyberattacks have been fully confirmed to hurt infrastructure.

If nine out of the 55,000 substations in the country broke down, the US could experience a blackout for up to 18 months (Thomson, 2017). The grid shutting down for this kind of extended time would require serious destruction to the equipment. Realistically, this kind of destruction is way more prone to animal damage than human damage. The takeaway is not to waste money and time on trivial problems humans may find serious (like solving air-gaps in software), but to actually take a look outside and fix the physical hardware interacting with the real world. Having a power outage can be the most disrupting event, so maintaining a working electrical grid is important for keeping people's lives electrified. Whether you care to admit it or not, squirrels are winning the cyberwar, so security officials should keep their eyes peeled for these bushy-tailed creatures.

References

- Barrett, Brian. "Are Squirrels a Bigger Threat to the Power Grid Than Cyberattack? Yes and No." *Wired*, Conde Nast, 3 June 2017, www.wired.com/2017/01/squirrels-may-beat-power-grid-glad-not-russia/.
- Bartels, Meghan. "6 Animals That Attacked Critical Human Infrastructure." *Business Insider*, Business Insider, 14 June 2016, www.businessinsider.com/animals-interfere-with-transportation-energy-science-2016-6.
- Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" *CSO Online*, CSO, 22 Aug. 2017, www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
- Gallagher, Sean. "Who's Winning the Cyber War? The Squirrels, of Course." *Ars Technica*, 16 Jan. 2017, arstechnica.com/information-technology/2017/01/whos-winning-the-cyber-war-the-squirrels-of-course/.
- Mooallem, Jon. "Squirrel Power!" *The New York Times*, The New York Times, 31 Aug. 2013, www.nytimes.com/2013/09/01/opinion/sunday/squirrel-power.html.
- MyRye. "Rye City Statement on Bowman Avenue Dam." *MyRye.com*, 21 Dec. 2015, www.myrye.com/my_weblog/2015/12/rye-city-statement-on-bowman-avenue-dam.html.
- Peterson, Andrea. "Are Squirrels a Bigger Threat to the Power Grid than Hackers?" *The Washington Post*, WP Company, 12 Jan. 2016, www.washingtonpost.com/news/the-switch/

wp/2016/01/12/are-squirrels-a-bigger-threat-to-the-power-grid-than-hackers/?utm_term=.24d92b20b8fe.

- Press, Associated. “Jellyfish Clog Pipes of Swedish Nuclear Reactor Forcing Plant Shutdown.” *The Guardian*, Guardian News and Media, 1 Oct. 2013, www.theguardian.com/world/2013/oct/01/jellyfish-clog-swedish-nuclear-reactor-shutdown.
- Soares, Marcelo. “Brazilian Blackout Traced to Sooty Insulators, Not Hackers.” *Wired*, Conde Nast, 21 Mar. 2018, www.wired.com/2009/11/brazil-blackout/.
- spacerog1. “35yrs Of Cyberwar, The Squirrels Are Winning - Shmoocon 2017.” *YouTube*, YouTube, 16 Jan. 2017, www.youtube.com/watch?v=cZPv-wro-O8.
- Tanriverdi, Hakan. “Die Tatwaffe Fehlt.” *Süddeutsche.de*, 19 June 2015, www.sueddeutsche.de/digital/tuerkei-ermittler-schliessen-cyberangriff-bei-pipeline-explosion-aus-1.2529345.
- Thomas, Cris. “Cyber Squirrel 1.” *CyberSquirrel1.Com*, cybersquirrel1.com/.
- Thomas, Cris. “Opinion: Squirrels Are Bigger Threat than Hackers to US Power Grid.” *The Christian Science Monitor*, The Christian Science Monitor, 6 Jan. 2016, www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0106/Opinion-Squirrels-are-bigger-threat-than-hackers-to-US-power-grid.
- Thomson, Iain. “What's the Biggest Danger to the Power Grid? Hackers? Terrorists? Er, Squirrels.” *The Register® - Biting the Hand That Feeds IT*, 19 Jan. 2017, www.theregister.co.uk/2017/01/19/biggest_danger_to_power_grid_is_squirrels/.
- Zetter, Kim. “Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report.” *Wired*, Conde Nast, 3 June 2017, www.wired.com/2011/11/water-pump-hack-mystery-solved/.’