MY WEIRD PROMPTS

Podcast Transcript

EPISODE #167

The Invisible War: Inside the World of State-Sponsored APTs

Published January 04, 2026 • Runtime: 24:54

https://myweirdprompts.com/episode/state-sponsored-cyber-warfare-apts/

EPISODE SYNOPSIS

In this gripping episode, Herman and Corn pull back the curtain on Advanced Persistent Threats (APTs), the elite, government-funded hacking units that play the ultimate long game in cyberspace, moving far beyond simple data breaches into the realm of permanent digital presence. From "living off the land" techniques that allow attackers to hide in plain sight using a system's own administrative tools to the high-stakes world of multi-million dollar zero-day exploits and complex psychological warfare, the brothers explore how nations like Russia, China, and North Korea utilize digital tools for diverse goals ranging from industrial espionage to the direct funding of national weapons programs. By examining the methodology behind attribution and the strategic "kill switches" embedded in global infrastructure, this discussion provides a sobering look at how the digital frontlines have shifted, explaining why the most dangerous threats are often the ones that have been quietly observing from inside the network for years.

DANIEL'S PROMPT

Daniel

"I'd like to discuss Advanced Persistent Threats (APTs) and their association with nation-state actors. What are the typical signatures or footprints that allow cybersecurity analysts to identify an APT and link it to a specific group? How do these groups manage to remain undetected within sensitive networks for long periods of time, and which states are currently the most active in this domain of offensive cybersecurity?"

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. I am Corn, and I am sitting here in our living room in Jerusalem with my brother.

Herman

Herman Poppleberry, at your service. It is a beautiful day outside, but we are about to dive into some pretty dark corners of the internet.

Corn

Yeah, our housemate Daniel sent over a prompt that feels like something straight out of a cold war spy novel, but for the twenty-first century. He was asking about Advanced Persistent Threats, or APTs, and how these nation-state actors operate. He actually called them APCs in his message, which is a common mix-up, but in the cybersecurity world, we are talking about APTs.

Herman

Right, and it is a fascinating distinction. When most people think of a hacker, they think of some kid in a hoodie or maybe a group of activists trying to deface a website. But APTs are a completely different animal. We are talking about professional, well-funded, highly disciplined teams, often working directly for a government or a military intelligence agency.

Corn

It is that persistence that really sets them apart, right? Daniel was curious about how they stay undetected for so long. It is not just a smash-and-grab.

Herman

Exactly. The persistence is the key. Most cybercrime is opportunistic. If a door is locked, the average hacker moves to the next house. An APT? They will sit outside your house for six months, learn your schedule, figure out which window has a loose latch, and then wait for a rainy night when they know the sensors are less effective. They are playing the long game.

Corn

And that brings us to the first part of Daniel's question about signatures and footprints. If these groups are so professional and so stealthy, how do analysts actually pin an attack on a specific group or a specific country? It seems like it would be incredibly easy to just leave a fake trail.

Herman

You would think so, and they certainly try. But there is this concept in forensics called Locard's Exchange Principle. It basically says that every contact leaves a trace. In the digital world, we look at what we call TTPs, which stands for Tactics, Techniques, and Procedures. Think of it like a criminal's signature style. One group might always use a specific type of custom-made malware. Another might always exploit a certain type of server vulnerability.

Corn

So it is less about a literal digital fingerprint and more about a pattern of behavior?

Herman

Precisely. It is about the methodology. For example, some groups have very specific working hours. If an attack is consistently being managed between nine in the morning and five in the evening in a specific time zone, say, Beijing or Moscow, that is a huge clue. Even the language used in the code can give them away. You might find comments in the source code or even just specific linguistic quirks in the phishing emails they send.

Corn

I remember when we were talking about mainframes back in episode two hundred seventy. We touched on how these old systems are often targets because they hold the crown jewels. When an APT goes after something like that, are they using tools that are commercially available, or is everything they do custom-built?

Herman

It is a mix, but the high-end groups have their own development shops. They have teams of engineers whose entire job is to write new, never-before-seen malware. These are called zero-day exploits because the software developers have had zero days to fix the hole. That is one of the biggest signatures. If you see an attack using a zero-day that would cost two million dollars on the open market, you know you are not dealing with a hobbyist. You are dealing with someone who has a government-sized budget.

Corn

Daniel also mentioned the recent news here in Israel about a group called Hanala, which is reportedly linked to Iran. They claimed to have breached the phones of several cabinet ministers. Daniel was skeptical, though. He was wondering if this is actually a sophisticated breach or just psychological warfare.

Herman

That is such a sharp observation by Daniel. In the world of offensive cyber operations, the lines between a technical hack and a psychological operation are very blurry. Sometimes, a group will claim they have breached a high-level target just to cause panic or to make a government look weak. They might leak some old data or spoof some messages to make it look like they are inside the network.

Corn

Right, because if you can convince your enemy that you are everywhere, you do not actually have to be everywhere to win.

Herman

Exactly. It is about eroding trust. But at the same time, we have seen very real, very damaging breaches. The trick for analysts is to separate the boastful claims from the actual technical evidence. With the Hanala case, analysts will be looking at the metadata of any leaked files, checking the command and control infrastructure, and seeing if the methods match known Iranian groups like APT thirty-three or APT thirty-four.

Corn

You mentioned command and control infrastructure. For the listeners who might not be familiar, can you explain how that works? Because that seems like a major way these groups get caught.

Herman

Think of it like a remote control. Once a piece of malware is inside a sensitive network, it needs to talk to its masters. It needs to send back the data it has stolen and receive new instructions. It does this by connecting to a server outside the network. Analysts can track these connections. If they see a government computer suddenly starting to talk to a random server in a foreign country at three in the morning, bells start ringing.

Corn

But surely these groups are smart enough to hide those connections?

Herman

They are. They use what we call obfuscation. They might hide their traffic inside normal-looking web traffic, like making the data look like someone is just browsing a news site. Or they might use a chain of compromised servers across multiple countries to hide the final destination. It is a constant game of cat and mouse.

Corn

It reminds me of our discussion on radio frequency hygiene in episode two hundred seventy-one. If you have any kind of unexpected signal or "noise" in your environment, it is a red flag. In a network, "noise" is just unexpected data packets.

Herman

Exactly! And just like in RF hygiene, the best defenders are the ones who know exactly what their "normal" looks like. If you know every single device on your network and exactly what it should be doing, the APTs have a much harder time hiding. But in a massive government network with tens of thousands of users, finding that one "weird" packet is like finding a needle in a haystack of needles.

Corn

So, how do they stay in there for years? Daniel was baffled by that. You would think that eventually, someone would notice something.

Herman

One of the most effective techniques is called "living off the land." Instead of bringing in their own fancy tools that might get flagged by antivirus software, they use the tools that are already built into the operating system. They use administrative tools like PowerShell or Windows Management Instrumentation. To a security monitor, it just looks like a system administrator is doing their job.

Corn

That is brilliant and terrifying. They are basically wearing the uniform of the people who are supposed to be protecting the system.

Herman

It is the ultimate disguise. They also move "laterally." They might get in through a low-level employee's laptop via a phishing email. Once they are in, they do not immediately go for the big data. They sit quiet. They watch. They steal credentials. They move from that laptop to a local server, then to a database, slowly climbing the ladder until they have administrative access to the entire network.

Corn

And at that point, they can basically delete the logs of their own activities.

Herman

Precisely. They can cover their tracks as they go. If they are careful, they can stay in a network for five, ten, even fifteen years. There have been cases where a company only discovered a breach because they were decommissioning an old server and found a piece of code that had been running since the early two-thousands.

Corn

That is a long time to have a guest in your house that you did not invite. Speaking of guests, let us take a quick break from our sponsors. Larry: Are you worried about the invisible eyes of the digital deep state? Do you feel like your data is floating out there in the ether, vulnerable to every prying nation-state actor? You need the Firewall Blanket. This is not just any blanket. This is a high-density, lead-lined, polyester-blend shroud for your router. Simply drape the Firewall Blanket over your internet box and watch as your signal drops to zero. If the signal cannot get out, the hackers cannot get in! It is the only one-hundred percent effective way to secure your home network. Does it stop you from using the internet? Yes. But does it stop the APTs? Also yes. The Firewall Blanket. Safety is just a heavy cloth away. Larry: BUY NOW!

Corn

...Alright, thanks Larry. I am pretty sure a lead-lined blanket is just going to overheat your router and probably start a fire, so maybe don't do that.

Herman

Yeah, I think I will stick to my encrypted tunnels and multi-factor authentication, thanks.

Corn

So, back to the serious side of this. Daniel asked about which states are the most active in this domain. He mentioned North Korea, which he thought was surprising given how isolated they are.

Herman

North Korea is actually one of the most fascinating players in this space. Most nation-states use cyber operations for espionage—stealing secrets, political influence, or prepping for a potential war. But North Korea uses it for revenue. Because they are under such heavy international sanctions, they have turned their cyber units, like the famous Lazarus Group, into a sort of digital bank-robbing crew.

Corn

Right, like the central bank heist in Bangladesh where they almost got away with a billion dollars because of a typo in the instructions.

Herman

Exactly! They also target cryptocurrency exchanges. It is estimated that they have stolen billions of dollars in crypto over the last few years to fund their weapons programs. It is a very direct, very pragmatic use of offensive cyber. They do not care about being "persistent" in the traditional sense; they just want the cash.

Corn

Who are the other big players? I assume the usual suspects.

Herman

Yeah, the "Big Four" are generally considered to be Russia, China, Iran, and North Korea. Russia is incredibly sophisticated. They are the ones who gave us the SolarWinds attack, which was a masterclass in supply chain compromise. Instead of attacking the government directly, they attacked the software that the government uses to manage its networks. It gave them a backdoor into thousands of organizations simultaneously.

Corn

That is the ultimate "force multiplier." You hit one target and you get access to five hundred.

Herman

It was brilliant in a terrifying way. And then you have China. Their focus for a long time was intellectual property theft—stealing blueprints for fighter jets, pharmaceutical research, or telecommunications tech. They wanted to jumpstart their own economy by skipping the research and development phase. Lately, though, they have shifted more toward long-term persistence in critical infrastructure.

Corn

Like power grids and water systems?

Herman

Exactly. Groups like Volt Typhoon have been found embedded in United States infrastructure. The goal there isn't to steal data; it is to have a "kill switch" ready if a conflict ever breaks out. If you can turn off the lights in a city without firing a single shot, you have a massive strategic advantage.

Corn

And then there is Iran, which Daniel mentioned. How do they fit into the hierarchy?

Herman

Iran is very active and has become much more sophisticated over the last decade. They often focus on regional rivals, but they also target Western infrastructure and political figures. They are known for being quite aggressive. If they get caught, they do not always back off; sometimes they just lean into it. They have been linked to several wiper attacks, where the goal isn't to steal data but to completely destroy the hard drives of the target.

Corn

It is interesting because Daniel brought up that point about psychological warfare. If a group like Hanala claims a breach, even if it is a minor one, it serves the purpose of making the target feel vulnerable. It is about the "aura" of the threat as much as the threat itself.

Herman

Absolutely. And we have to be careful as analysts and as citizens not to do their work for them. If we amplify every claim without verifying it, we are helping them spread their influence. That is why attribution is so important. When a company like Mandiant or CrowdStrike puts out a report saying "This is APT twenty-eight," they aren't just guessing. They are looking at thousands of data points, comparing them against years of historical data.

Corn

I remember back in episode two hundred seventy-two, when we were looking at how airlines control the skies, we talked about the redundancy and the "nerve centers." It feels like cybersecurity is moving in that direction—away from just having a firewall and toward having these active "nerve centers" that are constantly hunting for threats inside the network.

Herman

That is exactly the shift. We call it "Assume Breach." You don't assume your walls will hold. You assume the enemy is already inside, and you build your systems to detect them and limit the damage they can do. It is called Zero Trust architecture. Every single request, every single movement inside the network, has to be verified.

Corn

It sounds exhausting, honestly.

Herman

It is! It is a massive amount of overhead. But when you are dealing with actors who have the patience of a mountain and the budget of a superpower, you cannot afford to be lazy.

Corn

Daniel’s prompt also made me think about the second-order effects of this. If these nation-states are constantly probing each other, are we in a state of perpetual "gray zone" warfare? It is not quite peace, but it is not an open war.

Herman

That is exactly what most strategic thinkers call it. The gray zone. It is a space where you can inflict real damage on an adversary without crossing the threshold that would lead to a conventional military response. It is a very dangerous game because the "red lines" are not clearly defined. If a nation-state shuts down a hospital's power grid and people die, is that an act of war? We don't have a clear international consensus on that yet.

Corn

That is a chilling thought. We are basically writing the rules of engagement as we go.

Herman

We are. And the technology is moving faster than the diplomacy. That is why understanding these APT signatures is so vital. If you can't prove who did it, you can't hold them accountable. Attribution is the first step toward deterrence.

Corn

So, for the average person listening—not the cabinet ministers or the sysadmins—what is the takeaway here? Is there anything we can actually do, or are we just pawns in this giant game of digital chess?

Herman

It is easy to feel powerless, but there is a "herd immunity" aspect to cybersecurity. Most of these APTs get their initial foothold through simple things like phishing. They send an email that looks like it is from your boss or your bank. If everyone—from the janitor to the CEO—practiced good digital hygiene, these groups would have a much harder time getting in.

Corn

So, things like using a password manager, enabling two-factor authentication, and not clicking on weird links actually matter in the context of national security?

Herman

They absolutely do. You are making yourself a "hard target." APTs are persistent, but they are also efficient. If you make it too difficult for them to get into your account, they might move on to someone easier. You are essentially helping to protect the entire network by securing your little corner of it.

Corn

It is like what we discussed in episode two hundred fifty-eight about mesh networks versus wired connections. The more robust and redundant your individual nodes are, the stronger the whole system becomes.

Herman

Exactly. And also, stay informed but stay skeptical. When you see a headline about a "massive hack," look for the source. Is it a claim from a random group on Telegram, or is it a verified report from a reputable security firm? Don't let the psychological warfare part of the operation work on you.

Corn

That is a great point. The "weirdness" of these prompts often comes from that intersection of high technology and human psychology. Daniel really hit on something important there.

Herman

He really did. It is a rabbit hole that goes all the way down to the core of how our modern society functions. We have built our entire world on these digital foundations, and now we are realizing that those foundations are being constantly undermined by some of the most powerful organizations on earth.

Corn

It is a lot to take in. But I think it is better to understand the reality of it than to just ignore it and hope for the best.

Herman

Knowledge is the best firewall, Corn. Even if it doesn't come in a lead-lined blanket.

Corn

Fair enough. Well, I think we have covered a lot of ground today. We talked about what makes an APT "persistent," the signatures like TTPs and zero-days, and the big players like the Lazarus Group and Volt Typhoon.

Herman

And we touched on that gray area where technical hacks meet psychological operations. It is a complex world, and it is only getting more complicated as we head further into twenty-twenty-six.

Corn

Definitely. If you are listening and you found this interesting, we would really appreciate it if you could leave us a review on Spotify or whatever podcast app you are using. It actually makes a huge difference in helping other curious people find the show.

Herman

Yeah, it helps the algorithm realize that we are more than just two brothers and a sketchy advertiser talking to ourselves in Jerusalem.

Corn

And don't forget, you can find all our past episodes and a contact form at myweirdprompts.com. We love hearing your thoughts and your own "weird prompts" that you want us to dive into.

Herman

Thanks to Daniel for sending this one in. It definitely kept us busy researching all week.

Corn

It sure did. Alright, everyone. Thanks for listening to My Weird Prompts. Stay curious, stay skeptical, and for the love of all that is holy, don't buy a lead blanket for your router.

Herman

Until next time!

Corn

See ya.

Herman

Goodbye.

Corn

This has been My Weird Prompts. We are on Spotify and at myweirdprompts.com. We will catch you in the next episode.

Herman

Peace.

Corn

Peace. Larry: BUY NOW!