writeANGLE Distinguishing Content

Compute Power Hijacking – Article
Exclusive to Dark Reading

http://www.darkreading.com/attacks-breaches/harvest-season-why-cyberthieves-want-your-compute-power/a/d-id/1328088

Harvest Season: Why Cyber Thieves Want Your Compute Power

What is the hottest commodity cyber thieves are going after these days? Credit card numbers? Medical records? Politicians' emails?

Those may always be big, attractive targets. But more and more, attackers are surreptitiously going after unwitting organizations' *compute power.* That is what enables them to steal all those other things in volume and commit all manner of online crimes.

We're witnessing a resurgence in compute power hijacking – or what the thieves call "harvesting" – for a variety of nefarious purposes. A big driver is the trend toward ever-larger-scale data theft. Why break into an individual's laptop to steal one credit card number when you can break into a retailer's data center and steal millions? Another driver is the surge in crypto-currency mining, a rapidly growing source of illicit profits.

To pull off these ambitious capers – to ex-filtrate multiple terabytes of data at a time – requires enormous, institutional-strength computing power. To get it, the bad actors are targeting legitimate enterprise data centers across all industries and company sizes. Once sophisticated hackers gain a foothold within a data center, they can dwell undetected for months. Indeed, the average "dwell time" for a successful breach is around 150 days, according to Mandiant's 2016 M-Trends report. And hijackers need only a fraction of the host's computing power to carry out their schemes. Consequently, their harvesting goes unnoticed.

Uncovering a Hidden Mine

Here's an example of the damage hijackers can do. Last year, a mid-tier insurance firm came to our company with a problem. They suspected their data center had been compromised, but couldn't confirm it. We sent some analysts in to investigate. Sure enough, they had a problem – beyond their wildest suspicions. Not only had they been breached, but the attackers had set up shop, changed the firewall and DNS rules, and were running a massive botnet operation out of the data center. This upstanding and security-conscious company had become the unwitting "botlord" of some 10,000 machines worldwide.

Our team was able to shut down the operation and clean up the infected systems. In the process, we discovered what they were really doing and why they needed all that compute power – Monero mining.

Monero is a form of crypto-currency, a derivative of Bitcoin, that is advertised as "secure, private and untraceable." Monero or Bitcoin mining refers to the activity of discovering, capturing and processing Bitcoin transactions floating around the internet. It's effectively a competition that favors miners with the most computing power. Right under our customer's nose, the attackers were using the hijacked computing power to run a Monero mining bank to collect transaction fees.

The beauty – or curse – of harvesting compute power is that it can be used to fuel any kind of illicit online activity. This includes ransomware, for example, or denial of service attacks. A clever attacker can initiate a DDoS attack in one country using compute power from another, making the attack that much harder to trace and easy to deny.

Locks are No Help Once the Thief is In the House

So, what can enterprises do to protect their valuable computing power from hijackers? Perimeter defenses like firewalls and IPS are certainly essential, but compute harvesting is something that takes place within the data center, after the "walls" have already been breached. Organizations first have to face the fact that they can't stop every attack, and redirect some of their security efforts to vulnerabilities inside the data center.

And in today's highly virtualized, cloud or hybrid data centers, those vulnerabilities are often easy to exploit. Server and network virtualization, combined with ever-increasing traffic, network speed and server density have created an enormous visibility gap. Administrators simply cannot "see" what is going on deep in their data centers, at the process level. That's why sophisticated malware can move laterally almost indefinitely until it finds an opening.

Enterprises need to take new measures to secure assets within the data center from threats that have successfully breached the perimeter. There are a number of techniques gaining traction today that security teams can deploy to turn the tables on attackers.

Distributed deception represents a significant advancement over conventional "honeypots" planted as bait for attackers. In a true distributed deception platform, decoys placed throughout a network recognize any indication of suspicious activity immediately, engage with it and reroute it to a containment area for investigation and threat confirmation.

"Reputation analysis," or the ability to recognize something that simply doesn't belong, is another emerging threat detection tool. It typically relies on having access to a threat intelligence network that's tracking suspicious IP addresses, domain names or file hashes associated with known malicious activity – the cyber equivalent of a "wanted" poster or watch list.

Micro-segmentation refers to the ability to implement and enforce security controls around individual or groups of applications within the data center. Any policy violation automatically triggers an alert to initiate an investigation. Of course, this requires deep visibility into data center activity, down to the process level, which as we noted earlier is a challenge. With today's visualization tools, however, administrators can map their data center applications and processes, making micro-segmentation more practical and feasible for more organizations.

The infamous but colorful Willie Sutton reportedly said he robbed banks because "that's where the money is." Today, cyber hijackers are going after data centers because that's where the compute power is. It's a high-return hack – the power harvested can be used for crimes that pay exponentially. And the power can come from any type of business, so thieves can bypass high-security financial institutions and hit more vulnerable enterprises.

Thwarting such advanced threats requires rethinking data center security. It's no longer just about adding to an already over-populated and increasingly expensive security stack comprised of firewalls, IPS, URL filtering, AV protection, DLP technologies and the like. It's time to think "inside the box" – to protect data center assets from internal threats and prevent the data center from becoming the unwitting host to a monster straight out of "Alien."

About the Author

Dave Klein is Regional Director of Sales Engineering & Architecture at GuardiCore. He has over 20 years of experience working with large organizations in the design and implementation of security solutions across very large scale data center and cloud environments. At GuardiCore, David leads the sales engineering team in North America, assisting GuardiCore customers in architecture and implementation of advanced data center security solutions for the rapid detection, containment and remediation of security breaches.