Comment

The revolution of obfuscation for cybersecurity and threat intelligence

[redacted]

It's no secret that cyber threats are everywhere and growing stronger all the time.

The daily headlines are proof -- including recent news on the Shadow Brokers NSA breach and incursions at Siemens, Moody's, Equifax and many other organizations. Yet for all the attention, most government agencies and private companies remain vulnerable to attack.

Fixating on a threat, in other words, is not the same as fighting it. Indeed, a September 2017 Ponemon Institute survey found that while 84 percent of organizations worry about cybersecurity, nearly three-quarters were stymied in threat intelligence by a lack of expertise and overwhelming data volumes. Much of that volume comes from a 20-fold increase in recent years of digital exhaust -- the potentially sensitive data users leave behind on the internet that hackers can use to breach systems and databases. It's a challenging scenario that compromises the mission and drains the global economy of more than $450 billion annually.

[redacted]

Not all threat intelligence efforts are… intelligent

Any credible cybersecurity effort relies on active threat intelligence to examine vulnerabilities and bolster defenses. But the wrong *approach* to threat intelligence can spell trouble. As IDG's InfoWorld puts it, many security products and services on the market "don't work as advertised, leaving us far more exposed to malicious code than we know." There have even been instances of cyber threat intelligence services that inadvertently do more harm than good.

Hackers, for instance, have been known to silently observe -- like a fly on the wall -- as threat intelligence consultants test the organization's networks and processes for weaknesses. Because firewalls, VPNs and passwords are proven to be vulnerable to attack, these bad actors can gain network access and then literally stand back and take notes as a white hat assessment team does the legwork for them -- kicking the tires of a system in search of vulnerabilities.

Indeed, the shortcomings of firewalls, VPNs, proxy servers and other traditional secure access solutions are well documented: Authentication is easy to fake and governance is often lax, allowing users -- and those impersonating them -- broad access once inside.

The problem is getting worse as modern cloud environments and mobility solutions enable remote personnel, online customers and third-party vendors to interconnect ever more deeply with enterprise systems. Despite this, too many organizations remain reliant on access solutions that seem more secure than they really are.

How security through "obfuscation" works

Against this backdrop, smart leaders are learning to embrace cyber defense and threat intelligence solutions as flexible and sophisticated as the state-of-the art digital attacks that bad actors keep unleashing on them. Success is increasingly tied to the emerging best practice of anonymizing -- or *obfuscating* -- sensitive data and user information.

Obfuscation typically involves masking user and organizational data through a powerful "transit cloud" of encryption and IP hopping capabilities. In this scenario, a skein of complex pathways and directory nodes sends communications through multiple networking hops that scramble user, location, IP address and other data. This ultimately makes the users invisible, their location untraceable and their data unusable to potential threat actors.

One reason obfuscation works is that it doesn't just *limit* access to data; it also makes that data unintelligible in cases where unauthorized access is gained. To snooping eyes, for instance, a security consultant logging on in McLean, Va., may show up as a school teacher in Marseilles,

OMB Deputy director of management nominee clears committee

GSA kicks off e-commerce portal effort

Digital fellowship program is back and growing for 2018

The revolution of obfuscation for cybersecurity and threat intelligence

Most Popular Articles

The revolution of obfuscation for cybersecurity and threat intelligence

Agencies link reorgs with employee engagement

States can keep options open on FirstNet

When government gets it right

GSA kicks off e-commerce portal effort

France.

A private transit cloud is accessed via connection with an organization's specifically configured access nodes and its exit nodes provide connection to the "dirty" internet. For good measure, some robust systems even outfit those exit nodes with ongoing, random alterations to IP addresses -- imagine James Bond's changing license plate situated near your own digital tail pipe.

Safety in separation: keep threat intelligence off your network

As I mentioned, cybersecurity is only as good as your threat intelligence. That's why obfuscation and related cloaked services should rely on implementing a threat intelligence structure that's completely separate from the corporate network. Otherwise, you risk the fly-on-the-wall hacking scenario I described earlier.

Ideally, a separate cloud-based infrastructure would allow the organization to gather threat intelligence and store information in hidden data repositories that only designated analyst users can access -- without impacting customers, partner organizations and corporate networks.

Thankfully, advanced capabilities like this are already becoming a reality. For instance, the Department of Defense Cyber Security Strategy requires teams of personnel who are responsible for defending the DOD information networks, protecting priority missions and preparing cyber forces for combat. These teams defend the nation by seeing adversary activity, blocking attacks, and maneuvering to defeat them. Networking technologies that provide non-attribution capabilities are providing necessary anonymity in performing these operations.

Security-conscious industries in the private sector are taking similar steps, using networking technologies that provide anonymity, obfuscation and high levels of encryption. There are many use cases that can be tailored to meet specific requirements. Instead of relying on conventional methods that have proven inadequate, now is the time to reimagine your approach to threat intelligence and secure access.

Ideally, your approach should move beyond the inadequacies of firewalls, VPNs and other outmoded secure access solutions. It should embrace practical tools that are mobile and cloud-based. And it should include threat intelligence architectures that remain totally separate and obfuscated, with a level of security that keeps your valuable data from making its way into the wrong hands.