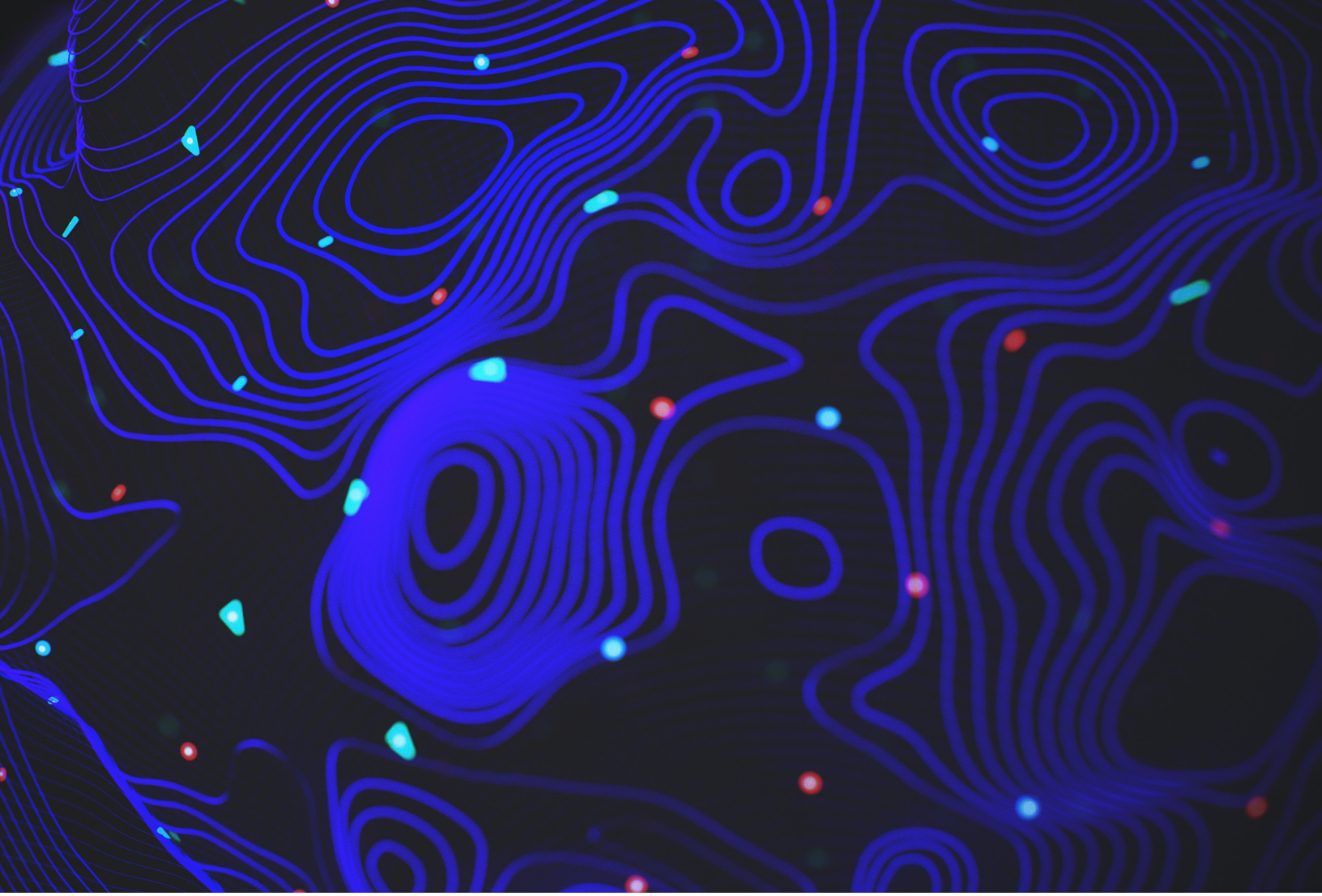
THREAT ACTOR BASICS: UNDERSTANDING THE 5 MAIN THREAT TYPES

WHITEPAPER

SentinelOne™

Contents



Introduction

Protecting the business in today's cybersecurity climate is all about staying up-to-date. Up-to-date with your security technology, up-to-date with security patches and up-to-date with the tools, techniques and procedures of different threat actors. In this post, we take a look at the five main threat types, how these adversaries operate and how you can defend against them.

1. Organized Crime – Making Money from Cyber

The number one threat for most organizations at present comes from criminals seeking to make money. Whether it's theft and subsequent sale of your data, flat out ransomware or stealthy, low-risk/low-return cryptojacking, criminals have been quick to adapt themselves to the opportunities for illicit moneymaking via the online world. There are digital equivalents of pretty much any 'analog' financial crime you care to think of, from kidnapping to bank robbery, and there's a double pay-off for the criminally-inclined: digital crime offers far greater rewards and much lower risks.

The low-risk factor is due both to the ability of criminals to hide their activity online and the ease of money laundering thanks to the rise of digital currencies. There are apparently over 17000 "Bitcoin millionaires" – addresses that hold more than $1 million worth of bitcoin – according to one report. As the value of bitcoin is currently on the rise again, expect to see some of those starting to cash out.

In the first 6 months of 2019, ransomware attacks have nearly doubled and business email compromises are up over 50% from the previous six months. It's not just the multinationals and famous names that are under attack either. Organizations from local governments to SMEs all represent soft targets for an increasingly experienced and well-equipped cybercrime underworld. Malware and ransomware kits are widely traded on the dark net and the impact is being felt. In the UK, 24% of SMEs reported an attack or cyber incident last year, amounting to a combined loss of over $10m.

How To Protect Against Criminals

To protect yourself from external threats like criminals, it is essential that your network and endpoints are protected by a modern, multi-layered intrusion detection and response solution. As proven by the number of successful attacks that hit the media on a weekly basis, the AV Suites of the past are simply antiquated and not up to the job of defeating well-funded cyber criminals armed with sophisticated tools. A modern solution should be able to detect anomalous behavior both pre-execution and on-execution and should have simple remediation and rollback capabilities to deal with ransomware and other threats.

Along with that, it's important that you patch vulnerabilities in a timely fashion. Criminals will soon jump on flaws like BlueKeep and although solutions like SentinelOne can detect exploitation of known vulnerabilities, timely patching is one more layer of defense that may persuade an attacker to look for an easier target.

An incident response plan is also a vital part of your security posture. Be sure that appropriate staff know what to do and who to contact in the event of a breach.

2. APT – Industrial Spies, Political Manipulation, IP Theft & More

Advanced persistent threat groups have become increasingly active as an estimated 30 nations wage cyber warfare operations on each others' political, economic, military and commercial infrastructure.

APT groups have proliferated in recent years, and tracking them is complicated. Groups may have common members and toolsets making attribution difficult, and often impossible. Added to that is the fact that security vendors do not use a common classification scheme, leading to a snowball of different labels for each group. Ever heard of Longhorn, Housefly or Tilded Team? Probably not, but they are all names for what is more commonly known as the USA's 'Equation Group'. A useful public document is maintained that tries to make sense of these different actors, their classifications and their activities.

Although APTs are primarily engaged in activities that benefit the interests of one country or countries over another, businesses can easily get caught in the crossfire, too. Whether it's a nation-state that wants your IP for their own use, cyber weapons like stuxnet that escape into the wild or weaponized zero-day vulnerabilities like Eternalblue, APT activity can have a dramatic impact on a business.

APTs aren't shy about straight-up financial theft either. North Korean APT groups like Lazarus (aka 'Hidden Cobra') have been engaged in SWIFT-related bank heists as well as targeting bitcoin exchanges.

Middle East actor 'Syrian Electronic Army' were widely held responsible for causing a $200 billion dollar loss on the Dow Jones stock exchange after an attack on the twitter account of the Associated Press. The hackers caused the stock market panic after using the hijacked account to tweet about a fake bomb attack at the White House, stating "Breaking: Two explosions in the White House and Barack Obama is injured".

How To Protect Against APTs

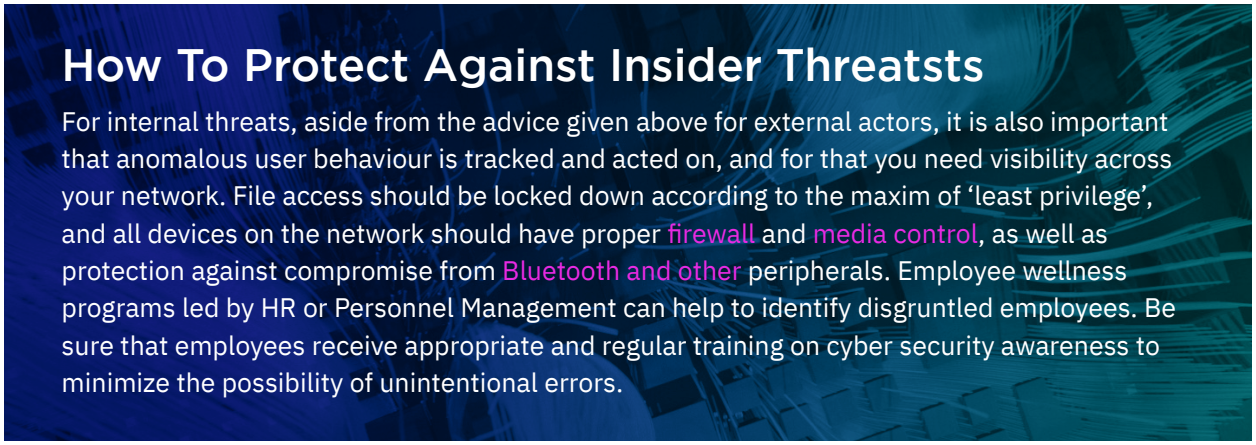
Defending against targeted attacks from APT groups requires similar defensive strategies to those mentioned above, but on top of that ensure that security risk assessment includes consideration of what assets your company may possess that would be attractive to nation states. Look at the TTPs of groups that might have an interest in your organization and devise suitable strategies around those.

For all external threats actors, be sure that employees are following safe password procedures and are aware of phishing techniques.

3. Insider Threats – Malicious Intent, Incompetence, Negligence

When valued employees go 'off the reservation', the impact to an organization can be devastating, and potentially far more catastrophic than the relentless attempts of external threat actors. It's common to think of insider threats as being a risk due to malicious intent, but as we've pointed out recently, negligence and unintentional errors can be as much, if not more, of a factor. Financial institutions like HSBC and Wells Fargo have both suffered embarrassing and costly data breaches due to unintentional errors.

At the other end of the scale, intentional insider threats are on the rise according to recent industry reports. These can be difficult to detect because employees may well have valid credentials and knowledge of the company's security procedures. Moreover, an increasing number of businesses are moving their data to the cloud where monitoring of user behavior and file access may be less rigorous or not yet in place. Staff being able to use personal mobile devices on the corporate network is also an area where organizations need to be increasingly vigilant.



How To Protect Against Insider Threatsts

For internal threats, aside from the advice given above for external actors, it is also important that anomalous user behaviour is tracked and acted on, and for that you need visibility across your network. File access should be locked down according to the maxim of 'least privilege', and all devices on the network should have proper firewall and media control, as well as protection against compromise from Bluetooth and other peripherals. Employee wellness programs led by HR or Personnel Management can help to identify disgruntled employees. Be sure that employees receive appropriate and regular training on cyber security awareness to minimize the possibility of unintentional errors.

4. Hacktivists – Rebels With a Cause, Or Maybe Just a Gripe

Like APTs, hacktivists like to pool their resources, but stealth is rarely on their agenda. Hacktivist groups aim to bring attention to an issue, person or organization that they want to positively promote or negatively disclose information about. Although less in the spotlight in recent years, groups like Anonymous and LulzSec have caused significant problems for businesses and organizations. The CIA, Sony Pictures and even governments such as the Philippines and Thailand have been targeted in the past.

Hacktivists tactics of choice include DDoS attacks on web services through botnets, defacing corporate websites, and taking over the Twitter and other social media accounts of high-profile individuals and businesses.

How To Protect Against Hacktiviststs

As we have seen, hacktivist campaigns will tend to target web services and applications, so it's important that as well as a modern security solution you have 2FA and MFA on all social media accounts, strong web application firewalls and a DDoS mitigation strategy that can analyse network traffic and identify anomalous requests. Be sure that your incident response plan includes mitigation strategies for reputational damage that could be caused by hacktivists.

5. Script Kiddies, Lone Wolves & Other Malcontents

Aside from the threats described above, there are also the dangers of individuals with no clear motives other than to break into other people's computers. These actors are sometimes labelled 'script kiddies', meaning teenagers who have acquired powerful tools written by others and deploy them against targets for fun or experimentation. However, that 'script kiddie' designation is not entirely accurate and also risks downplaying the seriousness of the threat from these kinds of actors.

A good example is the recent case of expert programmer and webstack engineer Paige A Thompson. For seemingly no reason, or at least not a reason that fits into the categories discussed above, Thompson allegedly hacked CapitalOne and other corporations causing data breaches that could cost the affected parties millions of dollars in FTC fines – such, at least, was the fate of Equifax – even though the data was not actually sold or distributed.

A different kind of case that would fall into this category would be a 'lone wolf' such as Phillip Durachinsky, the alleged developer of Fruitfly, malware targeting macOS that was used to infiltrate systems belonging to companies, schools, police departments as well as state and federal governments. Durachinsky's motives remain unknown.

How To Protect Against Script Kiddies et al

This threat actor type can be either internal or external. A good EDR solution should protect against non-targeted attacks like these. Anti-phishing strategies should also be in place here as phishing kits are as popular among script kiddies looking to see what they can 'catch' as they are among other threat actor types.

Conclusion

In this post, we've looked at the five main threat actor groups and some strategies that you should have in place to present an effective, multi-layered security posture. The modern cyber world has changed markedly from just a few years ago, with tools and techniques proliferating to the advantage of different kinds of attackers, from script kiddies to nation-state actors. If you would like to see how SentinelOne can help protect your organization against all kinds of threat actors, contact us for a free demo.