Applauding Active Directory Best Practices from Microsoft, and 3 More Expert Tips to Securing Intellectual Property

Microsoft recently released a whitepaper titled *Best Practices for Securing Active Directory* that spanned 314 pages; 72,000+ words detailing many (but certainly not all) "general categories of vulnerabilities" through Active Directory (AD). The whitepaper provides many scenarios for AD vulnerabilities where malicious operators penetrate the infrastructures of U.S. organizations and exfiltrate billions of dollars in intellectual property (IP) and undoubtedly, national security intelligence as well. Every InfoSec professional should have this document readily available as a point of reference for securing AD.

As InfoSec professionals, our job is to understand these types of threats and take the necessary precautions to secure the IT systems in our charge. But as you can see from the recent Microsoft 300+ page reference whitepaper, there are many considerations. Until recently, much of the problem with the IP theft intrusions described above has come from internal operators or negligence from careless users with greater permissions than their roles required. More recently however, groups of malicious operators are carrying out attacks based on the victim organization's political affiliation or recent activity that a "hacktivist" group didn't agree with.

Case in point is a recent attack on the governments of Syria and Saudi Arabia by the Anonymous hacktivist group "on the behalf of the people of Syria." Anonymous condemned the Syrian government and rebel fighters who received support from the Saudi government for civilian casualties.

Unfortunate as Anonymous-type hacks are, they are mostly inconveniences in the form of denial of service or attempt to publicly expose something about the victim organization that Anonymous disagreed with. Prime example here is the recent Anonymous attack on Bank of America for what Anonymous alleged was a massive spying operation by the financial giant.

The threats most detrimental to both Wall Street and our national security are the ones where the malicious operators seek to purge trade secrets and national security data. These industrial

espionage attacks are generally focused on transferring technology from companies that have spent billions on research and development to competitors through either private hacker-for-hire operations, or by nation states which use their military cyber-attack capabilities to steal the information on behalf of a company within their own country. Arguably billions of dollars – perhaps trillions – are stolen every year from public and private organizations just in the U.S. alone. A true quantification of IP theft however is unknown because of the PR nightmare that comes with the announcement "oops, our data was stolen."

Adding insult to injury are malicious operators working for nefarious governments that want our trade secrets and our national security data (for military advantage). In June of this year, Chinese wind turbine maker Sinovel was charged by the U.S. Department of Justice with stealing trade secrets from US-based American Semiconductor Corporation to the tune of $800 million. InfoSec experts estimate (on the conservative side) that in just this past year, China alone may have stolen $1.5 trillion in IP.

Your best defense is to attack the problem holistically: Here are 4 steps that will jump-start securing your IP Protection Strategy.

No, we are not saying these IP thefts are a result of Active Directory negligence nor its inability to block all avenues of intrusion. Proper AD policy alone won't prevent a malicious operator from stealing your IP. As InfoSec practitioners, what we have discovered over the years – much of it by trial and error – is that the following multi-pronged holistic approach works best:

1. Follow the guidelines Microsoft has outlined in Best Practices for Securing Active Directory. Make it difficult for the bad guys; they are looking for easy ways into your infrastructure.

2. Understand the entry points in your infrastructure that are the most vulnerable. Often last thought of in security awareness and compounded by BYOD, your most vulnerable infrastructure link is mobile device access.

3. Have an IT security information & event log management (SIEM) system in place that is alerts-based. Don't get caught sleeping. Use this SIEM system for proactive IT security management.

4. Incorporate hardware-separated multi-factor authentication (MFA) that validates the user at the software and hardware layers.

This holistic approach does not guarantee iron-clad and untouchable IT. Essentially, you are fortifying your infrastructure with multiple layers of technology surrounded by best practices that a hacker would find extremely difficult to crack through. A great place to start is the AD Best Practices whitepaper from Microsoft.

Start by shoring up your active directory policy per Microsoft guidelines.

IntegriCell believes Microsoft's best practice policy is very sound. Microsoft's 134-page reference whitepaper document is an all-encompassing library that discusses the most common AD attacks and recommendations to circumvent them. Microsoft's recommendations center around four basic constructs.

1. Understand how network infrastructures have been compromised in the past so that you avoid the same pitfall.
2. "Reduce the Active Directory attack surface" – as in minimize privileged access across the infrastructure and lock down domain controller access so the Active Directory database cannot be manipulated.
3. Monitor Active Directory for signs of compromise.
4. Develop response and recovery guidelines in the event of compromise.

We also believe that Microsoft is very much on target suggesting that "the most secure network is a well-administered one." You can't manage what you can't see and you can't see what you are not monitoring. In the most egregious of scenarios that Microsoft looked at where compromise took place, most of the victim organizations had been attacked long before the breach was discovered. And because of this lack of visibility, corrective action was delayed and most unfortunately, more IP was extracted from the victimized organization.

When you are a citizen of country A traveling to country B, you are the most vulnerable for having your mobile device and company data stolen.

Since most organizations use AD as the core of their identity and access management strategy, dedicating resources to protect this infrastructure is imperative. But, this brings up an important point; do those same organizations monitor how mobile devices interact with AD credentials, privileges and their use?

The 'bad,' the 'ugly' and the dirty little secret the cellular carriers don't want you to know about…

Malicious operators pick the low hanging fruit, and in today's massively complex network environments the asset that is always connected and always open, is your smartphone. What we mean by "always open" is always connected to the carrier network.

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 allows U.S. law enforcement to conduct criminal investigations through wiretapping of digital phone networks. According to the FCC website, "CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities." The act essentially obliges carriers to provide a back door for law enforcement to listen to any phone conversation on any cellular phone. At any point in time, with a keystroke your mobile device can be wiretapped. No special modification to your device is needed; it is built into the architecture of the device at the factory.

INTEGRICELL

The dirty little secret your wireless carrier wants to keep from you is the dangers of the international 'rogue' carrier network. When you are a citizen of Country A, traveling to Country B, rogue carrier networks make it possible for governments to take your information with almost no consequences.

This is the dirty little secret that your wireless carrier does not want you to know about. In fact, Verizon Wireless has a "Law Enforcement Resource Team" or LERT that is tasked with assisting law enforcement with all requests for information. LERT is there for law enforcement 24/7/365 to tap into your phone at any moment's time. To be clear, it's not Verizon's or AT&T's or any other US carrier's LERT…

US carrier LERT activity isn't the dirty little secret; this is just the *bad*. The *ugly* here takes place when you travel outside the U.S. with your mobile device. Because your device is always "open," you are vulnerable to any malicious operator posing as a valid international carrier network or seemingly safe WiFi hotspot. Here's one scenario:

Bill travels to Paris every other month to visit his EMEA sales team. On his last visit he connects to local carrier XYZ because he doesn't trust the WiFi at the local café. Bill VPN's into his network and works as normal for a Tuesday morning, conducts his business the next two days and flies home without intrusion incident. The next two weeks go by without incident, but the following week there is a breach and the source of the breach is traced to Bill's tablet.

This type of breach is not uncommon. Bill was hacked by carrier XYZ which was actually what we call a rogue carrier network. A malicious operator hacked Bill's phone, cloned it and sat quiet for nearly a month. Then out of the blue Bill's credentials were used to log onto the network and then hackers helped themselves to 2TB of company secrets. Good thing Bill's company wasn't a defense contractor with national security at stake. Sadly, however, Bill's company did not have a security information and event management (SIEM) system, which takes us to the next approach, protecting your IP.

Have a proactive SIEM system in place that alerts when a threat is detected

Had Bill's company had an event log management system in place with correlation capabilities, the IP lost could have been minimized or even averted entirely. The breach wasn't discovered until a performance glitch was discovered on the server that was being compromised. A 2TB download on a legacy server that wasn't fast in the first place bogged down some apps that were dependent on that IT asset. This performance issue was how the breach was discovered. But it wasn't until Bill's phone – er, clone – had hit the server for three days straight at 4:00 a.m. corporate headquarters' time.

An appropriate SIEM system with event log correlation would have revealed two significant threat indicators at the time of the initial breach. First indication: Bill's cloned phone initially accessed the network at 4:00 a.m. the first time, 3:00 a.m. the second time and 2:00 a.m. the third time, yet Bill has never accessed the network in the middle of the night when he is in the U.S. Second (correlated) indication: Bill's clone accessed the network from Saudi Arabia on two of those instances, but Bill was in Philadelphia every instance.

Bill's accessing the network in the middle of the night is not that much of an anomaly as a standalone incident. It happens. Had his company had event log correlation capability and correlated three middle-of-night logins with a login location 6,000 miles from

where he was that night, an alert could have been sent to the IT security admin to close the port that was accessed.

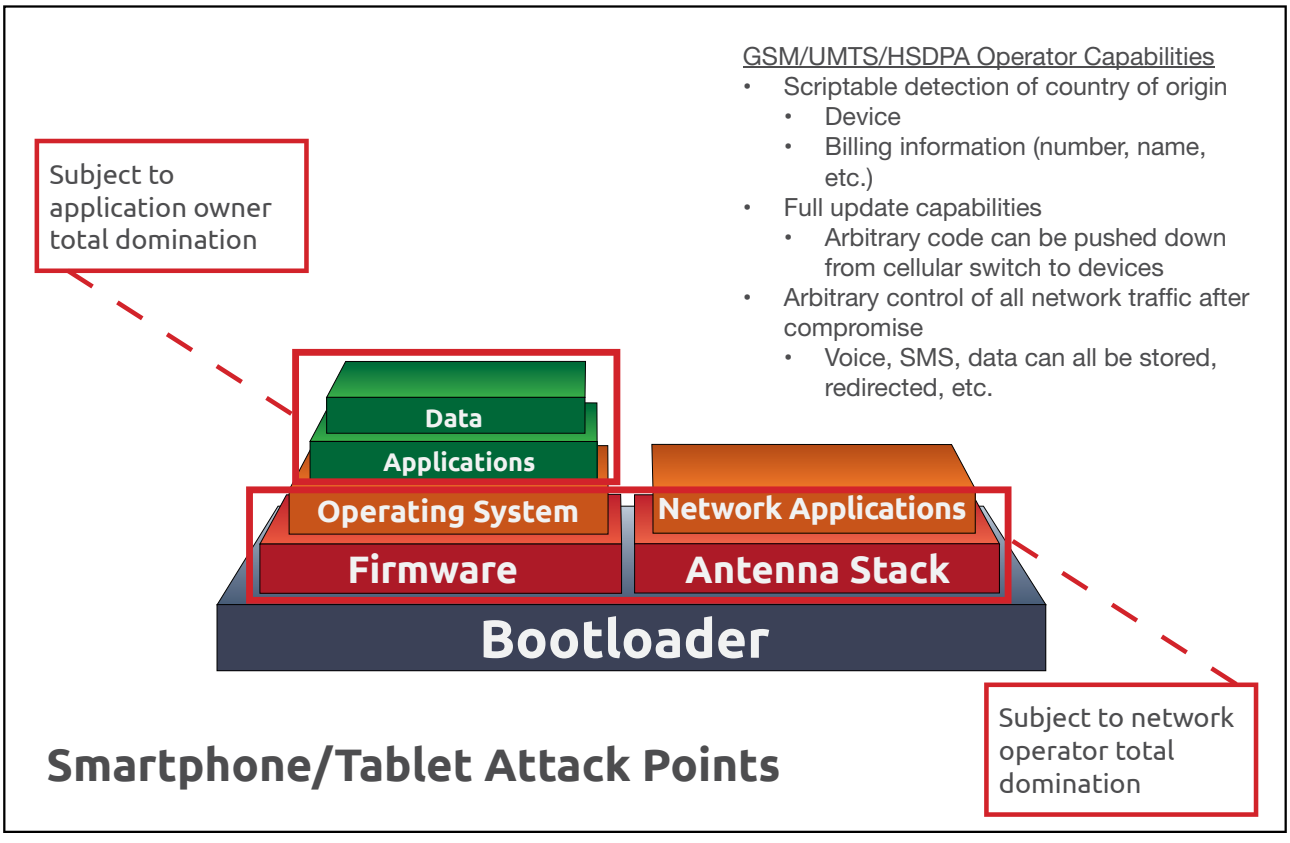
Additionally, when the FBI investigated the breach, Bill's company was unable to provide forensic log data on the first two intrusions because there was no SIEM system in place to track the log data for the server involved. Several IT analysts looked for the log data but it was erased after the first two breaches. After an exhaustive search of the server in question and dependent servers, they were able to find some log data but little to go on. Had a proper SIEM system been in place, the log data would have been preserved and encrypted for forensic analysis after the breach.

At the time of Bill's clone hack, there was nothing out of the ordinary according to Active Directory. It was the right device, with the right access credentials, so it had the right permissions to access the data it eventually exfiltrated. Had there been multi-factor authentication (MFA) in place however, access would have never been granted. Which leads us to the next approach…

MFA through hardware separation

Last but certainly not least in rounding out this holistic approach to protecting your IP is multi-factor authentication. Bill's "open" phone would have never been hacked by a rogue carrier had there been a higher-integrity authentication method that validated the user separately from the cloned carrier instance (and not just a simple username/password combination). This hardware separated validation would have authenticated Bill as the approved user for the device with a matching token key. The malicious operator would not have been able to validate carrier credentials plus the hardware-separated token, and access to the device and the IP on the network would have been denied.

The hardware-separated token device in this instance is called KeyLime from IntegriCell, and was recently unveiled at an InfoSec trade show. KeyLime is about the size of a wedge of lime and is easily stored in a laptop bag, purse, or small carry-on bag. The device only requires a 3.5mm, 4 conductor audio



jack which is standard on Android and iOS mobile devices. Simply plug the KeyLime device into the audio jack, authenticate your mobile device identity to KeyLime and your mobile device is locked down. More information about the KeyLime hardware device can be found at http://integricell.com/products/keylime/.

The significance of hardware-separated authentication cannot be understated, especially while traveling overseas. Any organization with international travelers should understand the risks associated with taking mobile devices out of the U.S. Malicious operators – some working for the governments of the countries your people are visiting — are deceiving mobile users who think they are on authentic carrier networks. Billions, arguably trillions, have been stolen in IP and national security secrets to these governments and their industrial espionage affiliates.

Conclusion

IntegriCell was founded to provide insight into the constantly-evolving threats that impact mobile technologies, and IP theft is a hugely-evolving development that we talk about frequently at speaking engagements and in our whitepapers. Malicious operators are coming at your organization from all angles and from places you never expected.

The Guardian Newspaper recently cited more than half a dozen internal U.K. government documents that allegedly revealed NSA-type covert surveillance on delegates at the 2009 G-20 Summit held in London. In addition to this alleged breach by U.S. ally, the governments of China, Russia, Saudi Arabia, Israel, and India have all been purported to have engaged in some type of covert telecommunications surveillance of its citizens and those of international travelers. And based on the breaches into organizations that we know about, we owe it to ourselves as InfoSec professionals to learn as much as we can about this type of intrusion.

We will never stop all IP theft, be we can make it as difficult as possible for a malicious operator to hack the IP on our collective network infrastructures. But one fix – albeit Active Directory best practices, event log correlation or hardware separation – these days just is not going to be good enough. As IT leaders, CISOs need to educate themselves and their teams on the evolving threats we are seeing every day from clients. It is only by understanding the level of threat through education, that a higher sense of urgency will flood IT shops and organizations will become more security aware. It is these security aware organizations that are leading the charge and taking a more holistic approach to secure corporate and government IP.

Given what you know after reading this paper about rogue carrier networks, it's easy to see that the vulnerability of your IP is high, especially if you have international travelers. The number of mobile devices on your network is already difficult to manage because of BYOD (bring your own device) but when you factor in the general consensus among IT leaders that a mobile device is just a gadget that you get from a kiosk in your local mall and not generally a network workstation, and it's no wonder few organizations are truly security aware. So be more security aware, and put all hands on deck with a more holistic approach to fighting the bad guys. And if you need a partner advisor for shoring up your mobile device defense strategy, please give us a call.

Multi-factor Authentication (MFA) via the KeyLime hardware separation token.

INTEGRICELL

IntegriCell, Inc. | **www.integricell.com**

455 Massachusetts Ave. NW
Suite 430
Washington, DC 20001

Contact:
Phone: +1-208-360-3746
E-mail: contact@integricell.com

Fax: +1-208-621-3947
Support: support@integricell.com