Aite PARTNER. ADVISOR. CATALYST.

IMPACT BRIEF

OCTOBER 2020

Steve Hunt
+1.617.447.1948
shunt@aitegroup.com

Fixing Vulnerabilities in Active Directory and Kerberos

When one thinks of cybersecurity attacks, one thinks first about phishing, ransomware, denial-of-service attacks, and other headline-grabbing threats. However, nestled deep in most networks is an Achilles' heel. It's such a popular destination for attackers that network security, endpoint security, and cloud security vendors make it their prime directive to catch bad activities before attackers reach this enticing target.

The place all attacks seem to be worming their way toward is Active Directory. Microsoft's Active Directory is the treasure trove of all privileges and credentials—the master key that unlocks every account, every server, every bit of valuable data—and its lack of intrinsic security is legendary. While financial institutions are very familiar with locking important assets in a vault, the network's vault at those same institutions remains unlocked.

This Impact Brief, drawing from six interviews with heads of cybersecurity and risk management at large financial institutions in the U.S. and Europe, aims to help business and technology managers understand and mitigate a critical vulnerability.

THE PROBLEM

It's no secret that protecting organizations from cyberattacks is complex. New threats emerge all the time, and well-worn attacks get reused in innovative ways. Security teams at financial institutions erect defenses against criminals, terrorists, fraudsters, and identity thieves knowing that, sometimes, one or two will slip through the layers of protection. Attacks come in all shapes and sizes—computer hackers looking for bragging rights, businesses attacking competitors, rings of criminals stealing personal and financial data, or foreign adversaries looking to gain access to information.

Attackers are bold. It's rare that they get caught and punished. More than 93,000 cybercrimes in the U.S. were reported to the FBI in 2019, but one unit chief believes the number of unreported cybercrimes is likely 10 times that number.[1] Instead, attackers approach each network like it's a video game with levels to beat and treasures to unlock.

Aite Group spoke to six executives at large financial institutions in the U.S. and Europe to understand to what extent financial institutions bear the brunt of these attacks. All six felt that financial institutions and their customers are favorite targets for attackers, who just need to beat a few levels in the cybersecurity game. If attackers can compromise the organization's critical controls, they can move freely and take whatever they can carry.

Organizations' critical control infrastructures are aging, poorly staffed, misunderstood, and largely unprotected—leading to devastating losses. Executives Aite Group interviewed described Active Directory as the critical infrastructure or "beating heart" of the institution's connectivity. According to a 2020 report from Verizon, attackers smash a path toward Active Directory on nearly every attack other than a denial-of-service attack. Stealing Active Directory credentials is the perfect complement to ransomware and Trojans, and the threat is most frequently delivered by malicious email links or direct installs.[2]

The story of NotPetya illustrates the costs of a poorly protected critical control infrastructure. Launched in June 2017, NotPetya was one of the most destructive cyberattacks in recent years. It came in the form of a ransomware worm, tearing through Ukraine, Russia, the rest of Europe, and the U.S. Disguised as a software update but secretly carrying a Mimikatz-based hack collecting thousands of sensitive records, such as authentication credentials and password hashes, it moved laterally at high speed through shared network drives. As WIRED's Andy Greenberg reports, NotPetya alone led to the paralysis of thousands of computers at companies like Maersk, Merck, and FedEx, and is believed to have caused well over a billion dollars in

1. Steve Morgan, "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cisco and Cybersecurity Ventures, February 26, 2019, accessed October 6, 2020, https://cybersecurityventures.com/cybersecurity-almanac-2019/.

2. "2020 Data Breach Investigations Report," Verizon, accessed October 8, 2020, https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

damages.[3] Mimikatz quickly became the preferred tool to crack open Active Directory domains like walnuts.

Mimikatz is an open-source software application available on GitHub that extracts sensitive information. It has been linked to hundreds of cyberattacks. Verizon's 2020 Data Breach Investigations Report blamed Mimikatz-like credential dumpers for more successful breaches than any other attack tool.[4]

Attackers are not the only ones to use Mimikatz. Security teams routinely use Mimikatz and another tool, Bloodhound, for analyzing Active Directory and testing the quality of their own critical control infrastructure. For example, a few members of one very large U.S.-based bank's security team uses these tools weekly to see if they will defeat or bypass the bank's security controls. Attackers use them the same way, first by exploring the network and then extracting information about users, groups, domains, and domain controllers. Armed with details about the network's critical control infrastructure, attackers systematically commandeer it.

WHAT CAN BE DONE ABOUT IT

Why is Active Directory so vulnerable? It is the central repository of credentials and privileges—the place every system goes to open, connect, and share information. Its sole function is to make information available. It is also complex, with many moving parts and many ways to be configured, leaving lots of chinks in its armor for wily attackers to exploit.

Plus, it suffers from too many cooks in the kitchen. Active Directory is managed by administrators, the most powerful roles in a network. With administrator credentials, no destination or information is off limits. Each of the chief information security officers interviewed for this Impact Brief confessed they wrestle with having too many administrators. It starts innocently enough. Over time, some people are granted administrator privileges for temporary projects, then those privileges are never revoked. Sometimes former employees retain administrator credentials long after they've left a company. And occasionally, regular credentials, the day-to-day login credentials of regular users, are inadvertently placed in a domain administrator's group, elevating their power.

Finally, individual workstations may have local administrator access, or individual users may be logged in as local administrators. If so, those computers, browsers, and email accounts are all connected in a special and potent way to the domain controllers. If I were an attacker, I'd start with that workstation or individual by producing a counterfeit Kerberos authentication ticket.

Kerberos is a computer network authentication protocol. It's like a very busy box office handing out tickets. Only, these tickets are used for computers to connect to other systems around the network. Counterfeit tickets are a big problem and played a central role in the NotPetya attack.

3. Andy Greenberg, "He Perfected a Password-Hacking Tool—Then the Russians Came Calling," Wired Magazine, November 2017, accessed August 2020, https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

4. "2020 Data Breach Investigations Report," accessed October 8, 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Common and advanced attacks have names like pass-the-hash, pass-the-ticket, skeleton key, and Kerberoasting. Advanced attacks include Golden Ticket, DCSync, DC Shadow, and Silver Ticket.

For example, an attacker may use the Kerberos package module to gain access to any desired domain and groups; the attacker may wish to take over the account of a legitimate user, such as username Frank in domain 500, in such and such groups, setting the lifetime of the Golden Ticket for 10 days or 10 years. Similarly, an attacker may use the notorious DC Shadow attack to create a fake domain controller and then push changes to legitimate Active Directory domains via replication.

Microsoft quickly patches its related vulnerabilities, but Kerberos remains vulnerable because it doesn't keep track of the tickets it issues. This "statelessness" of Kerberos is like a problem networks suffered in the 1990s when firewalls did not keep track of traffic coming and going. It was easy for fraudulent network packets to piggyback on legitimate traffic until Check Point developed its stateful packet inspection firewall.

Solving these problems would involve somehow managing the state of every ticket and verifying that every transaction of an Active Directory domain controller correctly follows the Kerberos protocol in near real time. Security executives to whom Aite Group spoke pointed out that behavioral analysis in the cloud may be too slow to catch privilege escalation before it does damage. Therefore, they seek a deterministic solution based on straightforward rules.

Executives described the keys to solving the problem:

- Detect and respond to Kerberos attacks in near real time.
- Find and identify all domain controllers on the network, especially ones not in the inventory.
- Correlate Kerberos-related activity with Windows event logs and other network events.

Following standard cybersecurity practices may not adequately protect Active Directory. Conventional cybersecurity architecture commonly looks like the layers of an onion. Network protections, such as firewalls, stand sentry at the outer edge, while protection and detection software keep watch over endpoints, such as laptops and servers. Security information and event management (SIEM) collects suspicious activity around the network, and security orchestration, automation, and response (SOAR) products launch automated responses. However, none of these security solutions detects or responds to Active Directory attacks without human involvement.

Hardening Active Directory is another tactic for protecting critical infrastructure. In the Kerberos protocol, once a user or attacker has obtained someone else's granting ticket, the attacker can always go back to the issuing authority and get a ticket for a new service. Hardening that exchange, and controlling and monitoring it for misuse, is tricky using standard approaches. The attacker is going to be able to obtain and reuse a session identifier on the client for as long as that session is valid. Therefore, the only real answer to the session reuse problem is strong handling of the session.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Back in 2008, Microsoft engineers were already educating users on what to watch out for. Pass-the-hash was already rearing its ugly head in those days. Microsoft published guidance to security teams to turn on the audit function on endpoints and look for certain telltale event IDs.

It was, and remains, a well-understood vulnerability, and Microsoft has now built a rich audit capability into the client to audit and identify pass-the-hash-type attacks. So, if an organization has a strong audit policy and is sending logs to the SIEM, it can rapidly respond to such attacks. Adding SOAR tools to the equation can speed up response too, so the attacker doesn't have enough time to do anything malicious between getting the ticket and the death of the process. This will work if the security team can get the detection response and mitigation down to seconds.

It is possible to install technologies and pray that they fix the problem, but it's a question of maturity. Getting the alert to the security operations center and responding to that alert can still take an hour or longer in the companies Aite Group interviewed. If, on the other hand, the incident response process runs like a well-oiled machine, then technology can carry the ball across the goal line. Unfortunately, all of these measures will fall short of identifying when some transactions skip parts of the Kerberos protocol, or when imposter domain controllers pop up. Even more damaging is the difficulty of identifying and correcting the network's one-way and two-way trust relationships with outside parties.

SOLUTION

It makes sense, once it's clear that Active Directory is the jumping off point for so many attacks, that security executives should address Active Directory and Kerberos authentication vulnerabilities and work backward from there. Active Directory and Kerberos are, after all, systems establishing trust. In the spirit of zero trust (a philosophy extending oversight to every critical system in a network), these systems would have to be monitored and protected more diligently, validating the integrity of each part, including critical control infrastructure.

Security teams will have confidence in the critical control infrastructure when they can manage the state of Kerberos sessions, regulating when and how they are issued and revoked, monitored, and recorded.

One vendor stands out with the most Kerberos-focused solution on the market. Founded in 2015 and headquartered in Reston, Virginia, QOMPLX aims to provide a different type of protection against advanced attacks. The company's cyber product performs detection, monitoring, and response to protect critical control infrastructure. Its proprietary Kerberos software finds problems associated with privileged user account configurations, stale or outdated user accounts and machines, weaknesses in policies, and other risks. Most importantly, it takes an essentially stateless system that doesn't keep track of the tickets it issues and layers on "stateful" protection.

QOMPLX approaches the problems of critical infrastructure protection by closely monitoring and defending the most critical asset in a network: Active Directory. From this vantage point, the software can improve security of many other security systems. For example, watching and

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

managing Active Directory activity sends to SIEM or SOAR systems the following accurate real-time data:

- The state of Kerberos tickets
- Configuration parameters of domains, trusts, organizational units, group policies, and accounts
- Hygiene-related attributes, such as stale accounts and admin accounts without password expiration
- Activity and details about every operating system and IP address joined to every domain

Armed with this rich data, security teams can find, track, and stop attackers, and make the entire network more resilient.

CONCLUSION

- Active Directory is the heart of most financial institutions' critical control infrastructure. This infrastructure is aging, poorly staffed, misunderstood, and largely unprotected—leading to devastating, headline-grabbing losses.
- Attackers use highly automated attacks, such as pass-the-hash, pass-the-ticket, skeleton key, and Kerberoasting. Advanced attacks include Golden Ticket, DCSync, DC Shadow, and Silver Ticket. None are easy to spot or block using conventional methods.
- Standard security products and techniques, including SIEM and SOAR, do not mitigate the most damaging weaknesses, such as the statelessness of Kerberos tickets.
- QOMPLX provides a solution that can turn a vulnerable infrastructure into a resilient one.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

RELATED AITE GROUP RESEARCH

API Security: Best Practices for FIs and Fintech and Insurtech Companies, August 2020.

Ransomware Defense in Financial Services: Retreating From the Cloud, August 2020.

Making the Case for Identity and Access Upgrades, May 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com