QOMPLX:

ManyKatz: How Active Directory Hacks Went Mainstream

Active Directory and authentication protocols like NTLM and Kerberos are pillars of modern enterprise IT. They're also under attack. The story of how identity infrastructure attacks went from "Jedi" to "Just another Day at the Office" is 30 years in the making.

DES-474R

Mimikatz has been declared a "hacker's favorite tool[4]" and found its way into the toolkits of no fewer than 28 advanced persistent threat (APT) groups[5].

Introduction

For what started out as a coding exercise, the Mimikatz application may have earned, in the last decade, the application development world's "over achiever" award.

First released in 2011 by Benjamin Delpy, a French security researcher, the tool—the name of which means "cute cats" in French—was an excuse to test Delpy's programming skills in the C language, as Delpy explained to Wired in 2017[1]. It was also a way to demonstrate to reluctant experts at Microsoft that a flaw Delpy had discovered in Windows' handling of passwords was worthy of their attention.

When Cute Katz Attack

Within the small, exclusive and loosely coupled world of elite- and nation-state hackers, Mimikatz got noticed. Immediately. Delpy's new tool was among those used just a month after its release in the June, 2011 Operation Black Tulip[2], an attack on the Dutch Certificate Authority DigiNotar. That incident gave attackers the ability to issue their own, signed digital certificates for sites like Google. Those certificates then helped nation-state hackers harvest the email credentials and web browsing histories[3] for hundreds of thousands of Iranian citizens.

Mimikatz has been declared a "hacker's favorite tool[4]" and found its way into the toolkits of no fewer than 28 advanced persistent threat (APT) groups[5]. In 2017, an automated version of Mimikatz was embedded in the so-called NotPetya malware[6] that targeted government and private sector firms in Ukraine and across Europe. In one recent example, the security firm Symantec reported in June, 2019 that Mimikatz was among a clutch of publicly available hacking tools used by an APT group dubbed Waterbug to target governments as well as IT and communications firms and universities in South America, Europe, and Asia[7].

Like most every other successful piece of software, Mimikatz' has thrived because the application is accessible (free, actually) and does some important things very well. In particular, Mimikatz automates a variety of useful and powerful attacks against Kerberos, a widely used authentication technology that is in many Unix and Linux operating systems as well as Microsoft's Windows operating system and Active Directory.

1 https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/
2 https://www.cs.ru.nl/E.Verheul/SIO2019/black-tulip-update.pdf
3 https://www.rijksoverheid.nl/documenten/rapporten/2011/09/05/diginotar-public-report-version-1
4 https://www.adlice.com/hacker-tool-mimikatz/
5 https://attack.mitre.org/software/S0002/
6 https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine
7 https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments

DES-474R

Concern about data security and the perversion of data streams was part and parcel of the shift to "technology warfare.

Problems 30 Years in the Making

A pillar of modern network security, the Kerberos authentication technology was rounding its third decade of life by the time Mimikatz was first released. It was a byproduct of Project Athena, a 1980s-era experiment[8] to design a campus-wide distributed computing infrastructure at The Massachusetts Institute of Technology (MIT). Athena's purpose was to extend computing access to the broad student population, not to build a next-generation file security architecture. But project leaders soon realized that building the former required them to create the latter.

"It quickly became clear that it would be good to have security as part of the Athena Project, otherwise MIT students were going to embarrass you most days of the week," recalls Dan Geer, who was recruited to MIT from Harvard to help run Project Athena.

The system they designed took a cue from cutting edge work done in the 1970s and early 80s, including the Needham–Schroeder symmetric key protocol[9]. But the implementation of those ideas was novel and particularly well suited to the problem at hand: brokering security between users in a complex and ever-changing network environment.

Right place, right time

"Kerberos was the first authentication system you could get your hands on and for a while it was the only one you could get your hands on," Geer recalls. "And MIT gave away licenses to it, saying basically 'Have it. Play with it. Don't write home.'" The technology was a successor to NT LAN Manager (NTLM), a Microsoft protocol that was standard on Windows systems prior to Windows 2000. NTLM was, and remains, susceptible to trivial "replay" attacks where an observer can replay credentials shared on a network after listening in.

That was a boon to financial firms, recalls Geer, who launched one of the first IT consulting firms on Wall Street. "All these firms were replacing little green screens with Sun Workstations. Concern about data security and the perversion of data streams was part and parcel of the shift to "technology warfare." Kerberos provided an answer to those concerns, he said. "The Wall Street guys were quick to adopt it, and money was no object."

Between the interest of Wall Street firms, MIT's liberal licensing of Kerberos and the backing of technology giants like Microsoft, Kerberos adoption went forward "at flank speed," Geer recalls, with executives at large firms approaching him and his company to "Kerber-ize" applications. Financial firms have largely made the leap but some industries, including healthcare remain

8 http://news.mit.edu/2018/mit-looking-back-project-athena-distributed-computing-for-students-1111
9 https://en.wikipedia.org/wiki/Needham%E2%80%93Schroeder_protocol

In the nearly 30 years since Kerberos launch, attackers have perfected ways to exploit organizations' ubiquitous Internet access, while circumventing monitoring and security tools.

far behind financial services in implementing more secure authentication and deprecating NTLM.

Technology Debt

The strong embrace of Kerberos by the business and technology communities masked problems, however. While the mathematics girding the Kerberos protocol was impeccable, the implementation in Kerberos contained any number of problems that could weaken the security of the overall system, according to several security experts.

Kerberos was superior to pre-existing authentication methods like NTLM. But backwards compatibility with these non-Kerberos methods created exposures. "You have a lot of legacy components you just can't get rid of," notes Chad Tilbury, a Principal in the firm Forensic Methods and a senior instructor at The SANS Institute. "You have older authentication like NTLM that's used by legacy applications—it adds to the complexity," he said.

In theory, organizations can migrate off of those platforms and applications in favor of more secure alternatives. In practice, however, that rarely happens. "You have infrastructure with many people in it. You have people who have left or made modifications... I'm sure back in the lab in MIT, (Kerberos) was incredibly secure" said Tilbury. But to get it to work in practice, people had to make compromises. NTLM, for example, was easy to set up and ubiquitous. Despite being provably insecure, its use has lingered in legacy applications that have not become Kerberos or SAML-enabled.

Old Technology, New Attacks

By 2020, that technical debt was weighing heavily on enterprises, while attackers were taking full advantage of vulnerabilities created by years of security compromises.

In the nearly 30 years since Kerberos launch, for example, attackers have perfected ways to exploit organizations' ubiquitous Internet access, while circumventing monitoring and security tools. Today, spear phishing attacks on employees via email or web based attacks give malicious actors a foothold on networks. In the last ten years, the emergence of tool kits like Mimikatz, Metasploit, Impacket and Rubeus have empowered sophisticated and unsophisticated attackers alike, while growing their ranks.

Mimikatz, for example, made it easy to conduct "Pass the Hash" and "Pass the Ticket" attacks, retrieving specific "hashes" (or strings used to authenticate with NTLM Kerberos) from the memory or file system on a compromised computer, then re-using those values to access other computers in a network

One problem is that security tools that organizations rely on are ill-suited to modern attacks against platforms like Kerberos.

environment. Mimikatz also provides capabilities to "forge" fake Kerberos tickets that have never been issued – a related but distinct kind of attack from the pass the ticket or pass the hash attacks. "Prior to Mimikatz, these were 'artisan' level attacks," said Jason Crabtree, the CEO of the security firm QOMPLX. New tools have made them available to even novice attackers.

Attacks go from Days to Minutes

The widespread availability of tool kits has made the path from "proof of concept" to "push-button" access ever shorter. "Golden Ticket" attacks on Kerberos authentication systems were first demonstrated[10] by Mimikatz creator Delpy and Alva ("Skip") Duckwall in 2014 and immediately made available via Mimikatz.

They allow attackers to generate a Kerberos Ticket Generating Ticket (TGT), effectively giving them domain administrator credentials to any computer on the network for the life of the Ticket.

Newer tools with names like CrackMapExec, Bloodhound, DeathStar, Angry Puppy and Go Fetch make it easier than ever for attackers who can gain just a foothold on a target environment to quickly forge tickets, replay credentials, or map the plan to expand their control..

"A few years ago, it might take an attacker 24 to 48 hours to get full domain access using, mostly, trial and error," said Tilbury. "Now you have a tool that can audit the network in minutes and give you the exact path you need to get full access to the environment." Coupling together techniques like Kerberoasting with ticket forgeries can be a powerful means of lateral movement and privilege escalation – including for actors seeking to support mass ransomware deployments across enterprises.

Growing Challenges for Defenders

The growing accessibility of such attacks greatly complicates the work of defenders. "It is extremely challenging to spot these attacks," said Sean Metcalf, the founder and principal consultant at Trimarc, a security consulting firm. "Detecting forged Kerberos tickets is not trivial."

One problem is that security tools that organizations rely on are ill-suited to modern attacks against platforms like Kerberos. "We have a security ecosystem in which nothing is designed to work together," said Crabtree of QOMPLX.

10 https://www.slideshare.net/gentilkiwi/abusing-microsoft-kerberos-sorry-you-guys-dont-get-it

DES-474R

> *You can't assume that all users are legitimate users.*
>
> *Jason Crabtree*
> *CEO, QOMPLX*

"It's a hodge-podge, and that's true at every big (security operations center) I've walked in to."

And those security tools often have big blind spots. For example: "It's pretty easy to get past endpoint detection tools "by just renaming and/or re-compiling Mimikatz.exe," Crabtree points out. In fact, both black- and white hats have adapted Mimikatz to do just that: creating variants of it for specific use cases or deployment scenarios. A version dubbed PowerKatz, for example, is a version of Mimikatz rendered using PowerShell and was used in an APT-style attack on the Indian firm Wipro in 2019[11]. The firm CyberReason identified a variant that it dubbed "maybemini" that dispatches with the use of command line arguments[12] to evade command line auditing-based detection. Security tools that use heuristics to detect anomalies in Kerberos ticket information are also limited. Over time, attackers have developed ways of evading detection based tell-tale heuristics like ticket expiry times, encryption type downgrades and other meta-data.

Digging for Ground Truth

More fundamentally: security tools often make assumptions about what Crabtree of QOMPLX calls the "ground truth" of networked environments: how technology architects and managers think things work instead of how they actually work; a designer's intent versus as-built plans.

A great example: enterprise security controls and tools commonly assume that any upstream authenticated sessions can be trusted. "All these tools - including User Behavior Analytics (UEBA) solutions - assume that the traffic they're observing is attributed to a legitimate identity," Crabtree notes. However, tools for upending Kerberos authentication, such as Mimikatz clearly show that assumption should be questioned.

Identity attacks strike at the foundation that enterprise security controls, tools and services stand on top of. "You can't assume that all users are legitimate users," Crabtree said. "You can't assume that your behavioral detection tools, which are premised on a learned baseline that includes a malicious signal, will be able to detect that malicious signal."

The job of establishing ground truths is a challenging one for organizations—but of increasing importance. To manage the task, firms are increasingly turning to machine learning technology to tame massive data sets and dig deeply into fine grained activity on platforms relying on protocols like Kerberos. Addressing authentication for services which are "Kerber-ized" offers hope.

11 https://cyware.com/news/wipro-phishing-attack-was-conducted-using-screenconnect-and-power-katz-tools-indicates-new-intel-d3a7c00d
12 https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

> *The smartest organizations will find a way to leverage modern distributed systems and analytics platforms.*

However, organizations must also commit to stamping out protocols like NTLM which are provably insecure.

QOMPLX's software, for example, uses combinations of rules, statistics and machine learning techniques to pore over telemetry from network monitoring and security devices deployed across IT environments. Rather than simply flagging failed login attempts, for example, QOMPLX can verify that each Kerberos authentication event was correctly generated, issued, and traced to legitimate user interactions with the issuing domain controller. "What we do, fundamentally, is to make it hard to lie about authentication," Crabtree said. "By adding external state to Kerberos transactions instead of relying on heuristics, we validate the Kerberos protocol and the original design work done at MIT," he said.

The Future is Purple

The earthquake that began with the release of Mimikatz nine years ago continues, unabated. "Benjamin [Delpy] shocked the world when he released Mimikatz," said Tilbury. "But he's kept it up. Every three to six months there's an update. You get blown out of the water quarter after quarter." And that doesn't even consider the release and development of similar tools by other developers and communities.

In fact, risk is spreading. As computing moves from data centers to the cloud, technologies like Kerberos are being carried along with the tide. For example, many organizations are even connecting cloud authentication services for single sign-on (SSO) for SAML-enabled cloud services and linking them to Active Directory via Active Directory Federated Services (ADFS). That means that technology debt and underlying security risks are multiplying, not shrinking, across the almost limitless landscape of the cloud.

At his firm Trimark, Sean Metcalf says his clientele is going "all-in" on cloud platforms like Office365, GSuite, and platforms like AWS, Azure, and Google's cloud. Rather than simplifying their security challenges, cloud migration presents huge challenges for organizations as they look to manage identity and access across cloud and traditional IT environments, while also addressing the underlying security risks of legacy technologies like Kerberos.

The smartest organizations will find a way to leverage modern distributed systems and analytics platforms, enhanced by machine learning, to master the huge data sets that cloud deployments will engender, while integrating security operations more closely with development and IT management. Metcalf notes. "Security isn't going to be something that happens later," said Metcalf. "It can't be something you bypass, but just needs to be embedded in everything you're doing."

> *You're making a fundamental assumption that 'the sky is blue,' but have you looked?*
>
> *Jason Crabtree*
> *CEO, QOMPLX*

"Rather than hope for a break in the action, the security community needs to keep up" he said. "I still get a lot of blank stares. People haven't been punched in the nose with these tools." With all manner of attackers leveraging such platforms to attack Active Directory, NTLM, Kerberos, SAML and other identity infrastructure, security teams need to think and act more like attackers, using the same tools that they use.

He recommended creating security "purple teams" that combine the traditional work of red- and blue teams in a more interactive way, using data about possible attack paths and techniques to improve security in real time.

Crabtree of QOMPLX said that enterprises should shore up the security of their fundamental infrastructure like Active Directory, rather than throwing security tools at an environment in the hopes of "spotting something." They need to ensure that their authentication systems have not been subverted, and that their other security controls, tools and processes continue to operate as intended. Understanding the limitations of authentication protocols like NTLM, Kerberos, and SAML is essential for security teams in the modern federated enterprise. Kerberos has limitations but real-time analytics with external stateful validation means that Kerber-ized applications can still be authenticated with confidence. However, no analytics can offer similar levels of confidence for NTLM."Technology like QOMPLX's is no silver bullet," Crabtree notes. "But it is a way of re-building security operations on the bedrock of accurate data rather than the quicksand of flawed assumptions. There's just been a fundamental lack of scrutiny about where your data comes from," he said. "You're making a fundamental assumption that 'the sky is blue,' but have you looked?"

QOMPLX makes it faster and easier for organizations to integrate disparate internal and external data sources across the enterprise via a unified analytics infrastructure that supports better decision-making at scale. This enterprise data-fabric is called QOMPLX:OS, an enterprise operating system that powers QOMPLX's decision platforms in cybersecurity, insurance, and quantitative finance. Headquartered in Reston, VA, QOMPLX also has offices in New York, Denver, and London. More information about QOMPLX can be found at www.qomplx.com/.