thycotic

BLACK HAT 2018

HACKER SURVEY REPORT

BLACK HAT 2018

HACKER SURVEY REPORT

Based on a survey of attendees at Black Hat Conference, August 4-9, 2018

EXECUTIVE SUMMARY

Thycotic conducts a survey of hackers at the Black Hat conference each year to get their perspectives on vulnerabilities and attack vectors they find easiest to exploit. With nearly 70% of our 300+ survey respondents considering themselves "White Hat Hackers," the survey reflects a large proportion of attendees devoted to helping organizations stay safe by highlighting their surest wins for exploiting IT systems. That said, there were 30% of hacker attendees who anonymously admitted to potentially breaking the law in their hacking efforts. However, only 5% of respondents identified as pure "Black Hat Hackers" intending to compromise systems for malicious purposes or personal gain.

70%
Considered themselved White Hat Hackers

30%
Admited to potentially law breaking hacking

5%
Identified as Black Hat Hacker

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

KEY TAKEAWAYS

KEY TAKEAWAY #1:

Adopt a zero trust posture

Even with Microsoft investing heavily to improve cyber security, 50% of hackers say they easily compromised both Windows 10 and Windows 8 within the past year. Operating Systems are only as secure as the people using them, and the proper configurations applied. Knowing that compromise of user accounts is probably inevitable, organizations need a "zero-trust" posture that emphasizes least privilege to limit overprivileged accounts that give hackers wide and undetected access.

KEY TAKEAWAY #2:

Don't rely only on GPO for security

More than 90% of hackers say they compromised Windows environments despite the use of Group Policy Objects (GPO) to help maintain security and keep user privileges in check. Organizations should not rely solely on GPO for security. GPO and Microsoft tools must be augmented with other techniques and cyber security solutions to add multiple layers of security for a defense-in-depth strategy.

KEY TAKEAWAY #3:

Apply the principle of least privilege

Three out of four (75%) of hackers say companies fail at applying the principle of least privilege, giving user accounts too much access. Hackers confirm that organizations continue to give away too much access, especially local admin rights. Once compromised, these privileged accounts allow hackers to quickly elevate privileges to gain FULL ACCESS of the entire IT infrastructure and can remain undetected for long periods of time.

KEY TAKEAWAY #1:

Adopt a zero trust posture

Even with Microsoft investing heavily to improve cyber security, 50% of hackers say they readily compromised both Windows 10 and Windows 8 within the past year. Operating Systems are only as secure as the people using them, and the configurations applied. Knowing that compromise of user accounts is probably inevitable, organizations need a "zero-trust" posture that emphasizes least privilege to limit overprivileged accounts that give hackers wide and undetected access.

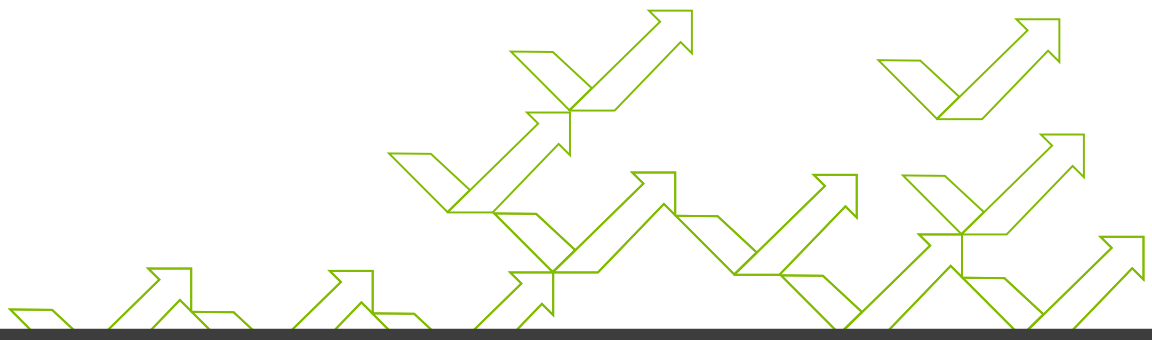
"Zero-Trust" is a concept that many organizations should use to build trust across their IT infrastructures using a Risk-based Model. When new devices are introduced onto the network---and before they obtain access to any other resources---they must first identity and verify themselves based on various security controls. The more sensitive the resources to be accessed, the more security controls they must satisfy. This introduces an adaptive security model that enables a business to maintain productivity while reducing risks from a cyberattack.

60%

OF HACKERS

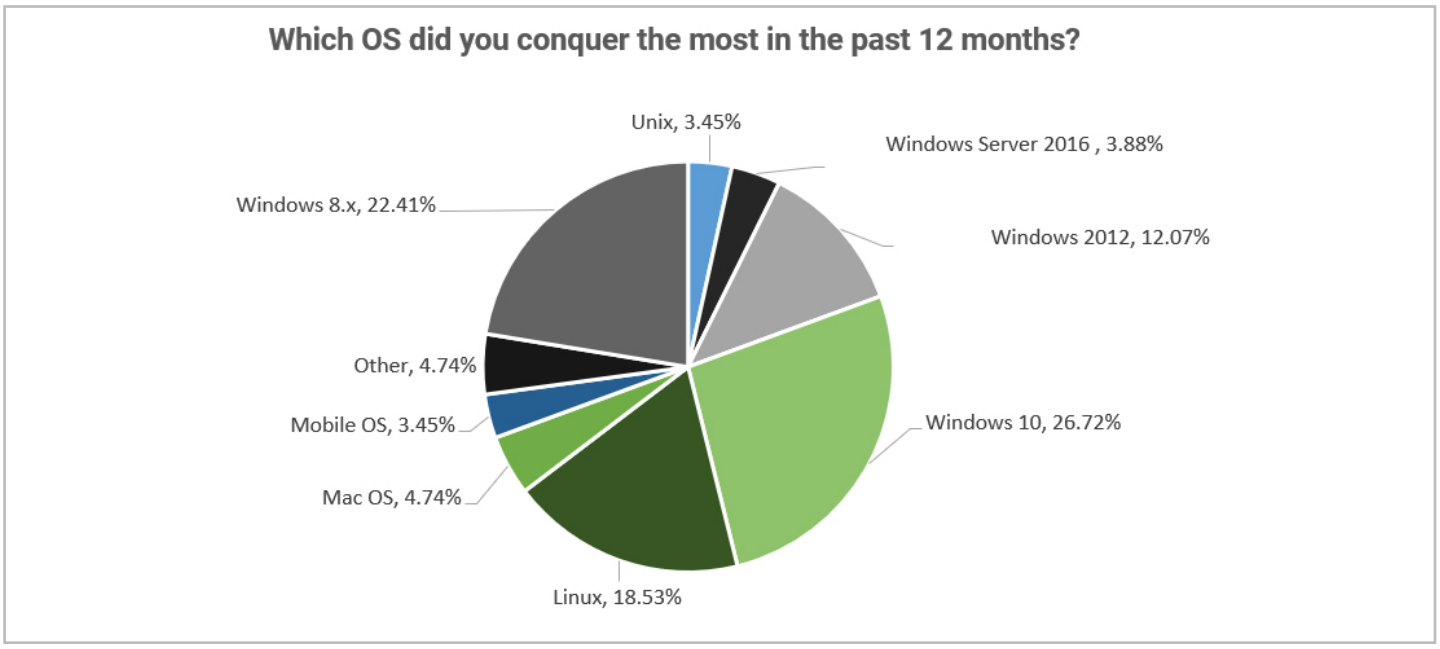
use social engineering as the fastest way to gain network access

Removing local administrative privileges, for example, provides the most effective way to protect endpoints from attack, with immediate, measurable benefits. Implementing and enforcing a least privileged security strategy, however, takes planning, collaboration, and tools that maintain the productivity of IT admins, desktop support, and business users.



SURVEY RESULTS

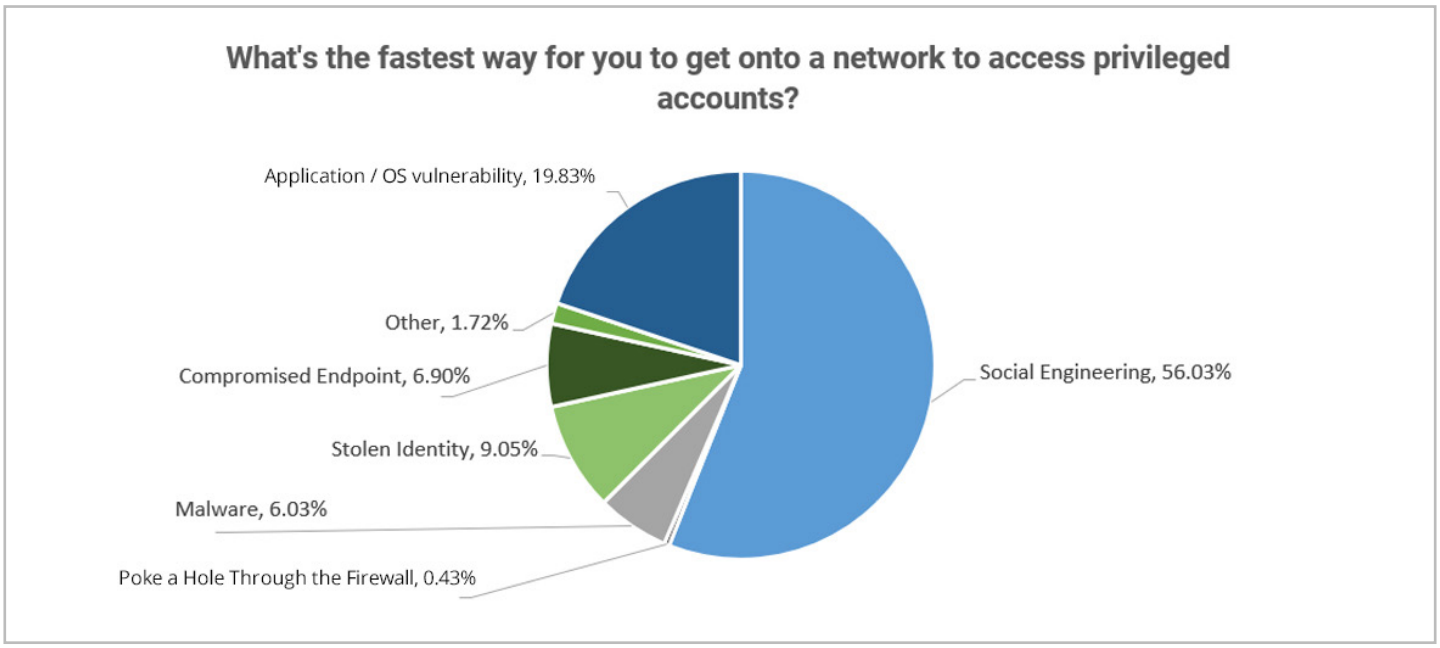
Windows 10 (27%) and Windows 8 (22.5%) dominated the systems hacked within the past year, with Linux OS (18%) also identified as easily conquered. Less than 5% of hackers listed Mac OS, Unix, and Mobile devices as compromised.



Unfortunately, hackers continue to exploit employees and misconfigurations across the IT environment.

While much attention is given to application and operating system vulnerabilities, zero-day attacks, and malware, hackers still find it much easier to trick users into simply handing over their corporate credentials. Once an attacker gains network access they can learn more about what software is being used, what patches are being deployed, when vulnerability scans are run, which systems and accounts have privileged access and how they can avoid detection.

Application and OS vulnerabilities remain a major problem, with almost 20% of hackers exploiting unpatched systems. Ten percent (10%) of hackers use identity theft to gain network access, with less than 7% using malware or stolen endpoints.



Password Re-Use is the Biggest Risky Behavior by Employees

We asked hackers to share an organization's biggest behavior-based security vulnerabilities – behaviors they exploit most often to access networks. Hackers confirmed that 50% of their exploits have uncovered employees re-using passwords that have been already exposed in other data breaches, giving hackers an easy way onto the network. These results confirm that employees constantly struggle with poor password hygiene. Once compromised, these end user accounts provide a ready pathway to privilege escalation by hackers.

RECOMMENDATIONS

Application control on server workloads, active anti-phishing and malware measures, and privileged account management are cited by Gartner as top priorities in 2018 to directly address the vulnerabilities highlighted in this Black Hat Survey.

With 85% of breaches involving compromised endpoints, it's clear that employees are still falling victim to social engineering schemes and poor password practices. A least privilege strategy with application control removes local administrative privileges on endpoints, enabling organizations to significantly reduce their attack surface and block the primary attack vector, preventing most attacks from occurring. Even if a user password is compromised, least privilege helps to limit the escalation of privileges that hackers rely on to get at sensitive information.

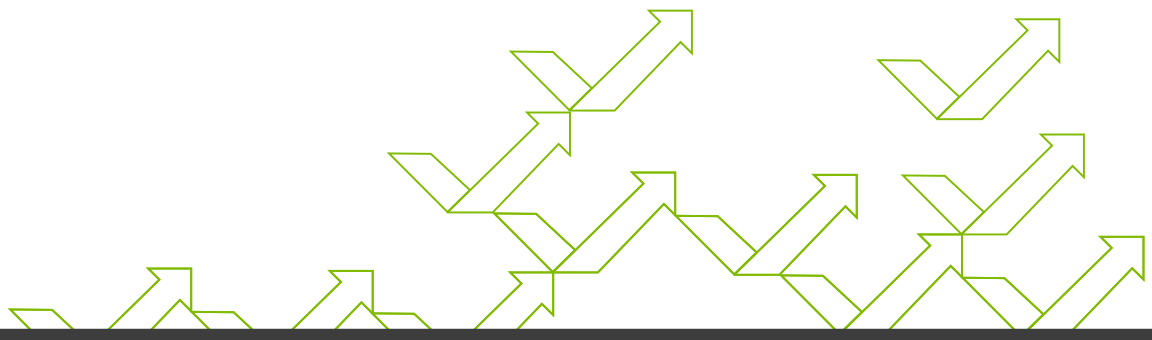
Using a Privilege Access Management solution also helps to minimize cyber fatigue while automating proper password practices for privileged credentials. It can keep employees from re-using poorly chosen passwords and save time for IT Ops and support desk teams

Learn more about how to implement a least privilege strategy with these resources.

Top 10 Tips to Successful Least Privilege Projects
thycotic.com/least-privilege-10-keys/

Free Least Privilege Discovery Tool
thycotic.com/least-privilege-tool/

Switching to Windows 10? Let's boost your endpoint security with a least privilege strategy
thycotic.com/windows10-least-privilege/



KEY TAKEAWAY #2:

Don't rely only on GPO for security

More than 90% of hackers say they compromised Windows environments despite the use of Group Policy Objects (GPO) to help maintain security. Organizations should not rely solely on GPO for security. GPO and other Microsoft tools must be augmented with other techniques and cyber security solutions to add multiple layers of security for a defense-in-depth strategy.

90%

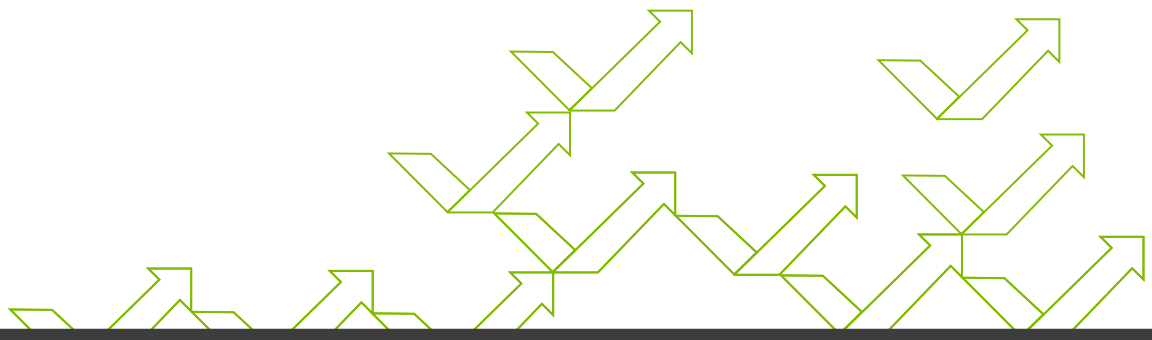
OF HACKERS

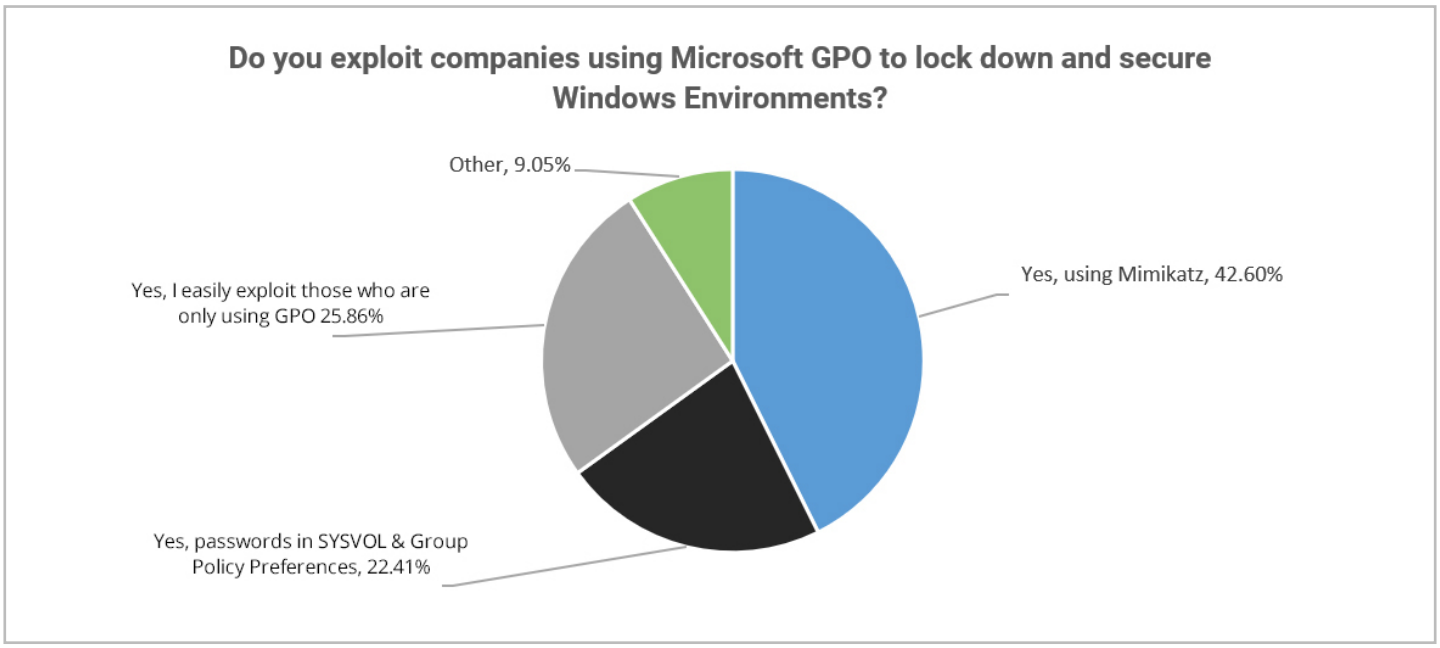
say they compromised Windows environments despite the use of Group Policy Objects (GPO) to help maintain security

SURVEY RESULTS

Many companies with Windows environments and Active Directory have been using GPO to centralize the management, configuration, and security of Windows domain-connected devices. GPO policies have been used to harden systems based on password complexity, configured users, network access, or restricted access to certain files and folders. Group Policies, however, rely on the devices being part of the domain, are voluntarily enforced, and must be network connected to get updates.

Despite using GPO to harden Windows environments, hackers indicate they can easily bypass security controls. Most hackers use Mimikatz, a popular Windows security audit tool (also available in Kali Linux), to extract plaintext passwords, hashes, PIN codes, Kerberos tickets from memory and perform pass-the-hash attacks. Other methods include getting passwords from SYSVOL, exploiting Group Policy Preferences or using Metasploit.





RECOMMENDATIONS

Organizations cannot rely on GPO alone to keep cyber criminals out of their networks. Security must should be augmented with other techniques and solutions for a defense-in-depth strategy.

Learn more with this whitepaper

Move Beyond GPO for Next Level Privilege Management
thycotic.com/least-privilege-10-keys/

KEY TAKEAWAY #3:

Apply the principle of Least Privilege

Three out of four (75%) of hackers say companies fail at applying least privilege, giving user accounts too much access. Once compromised these local domain accounts can allow hackers to exploit administrative privileges to gain FULL ACCESS of the entire IT infrastructure and remain undetected.

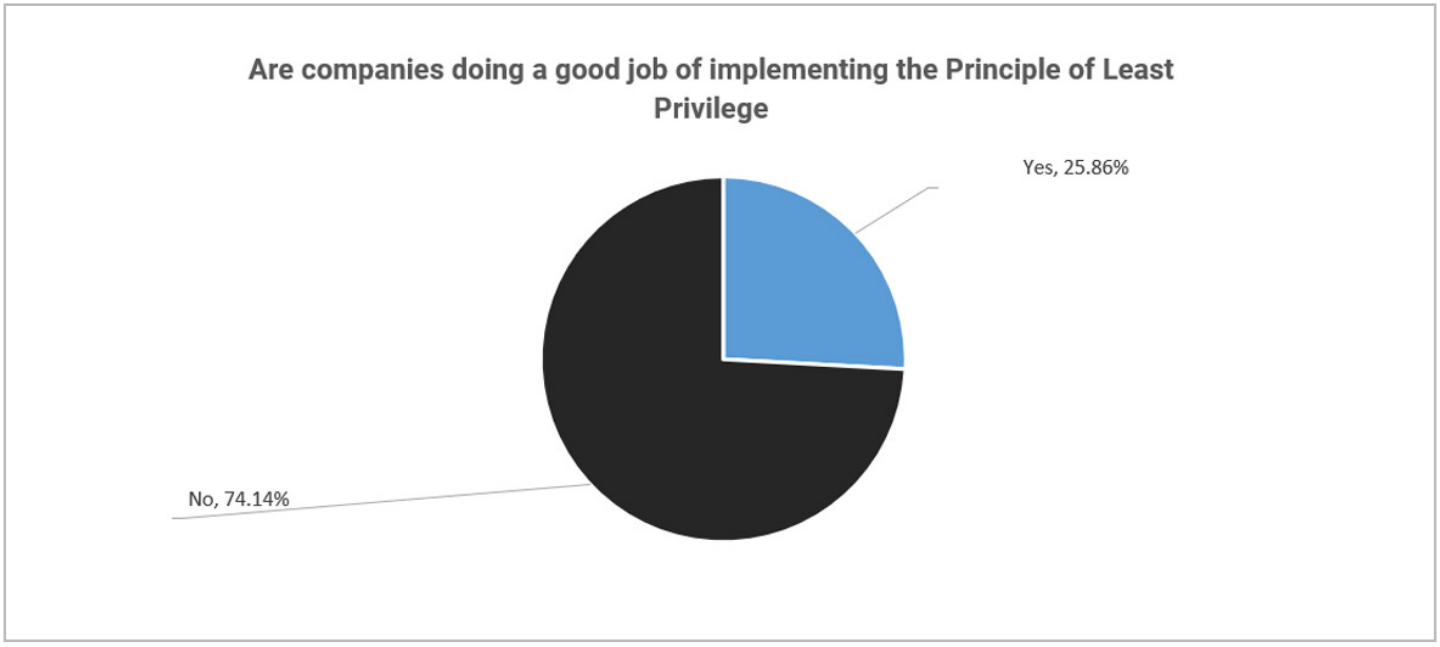
75%

OF HACKERS

say companies fail at applying least privilege, giving user accounts too much access

SURVEY RESULTS

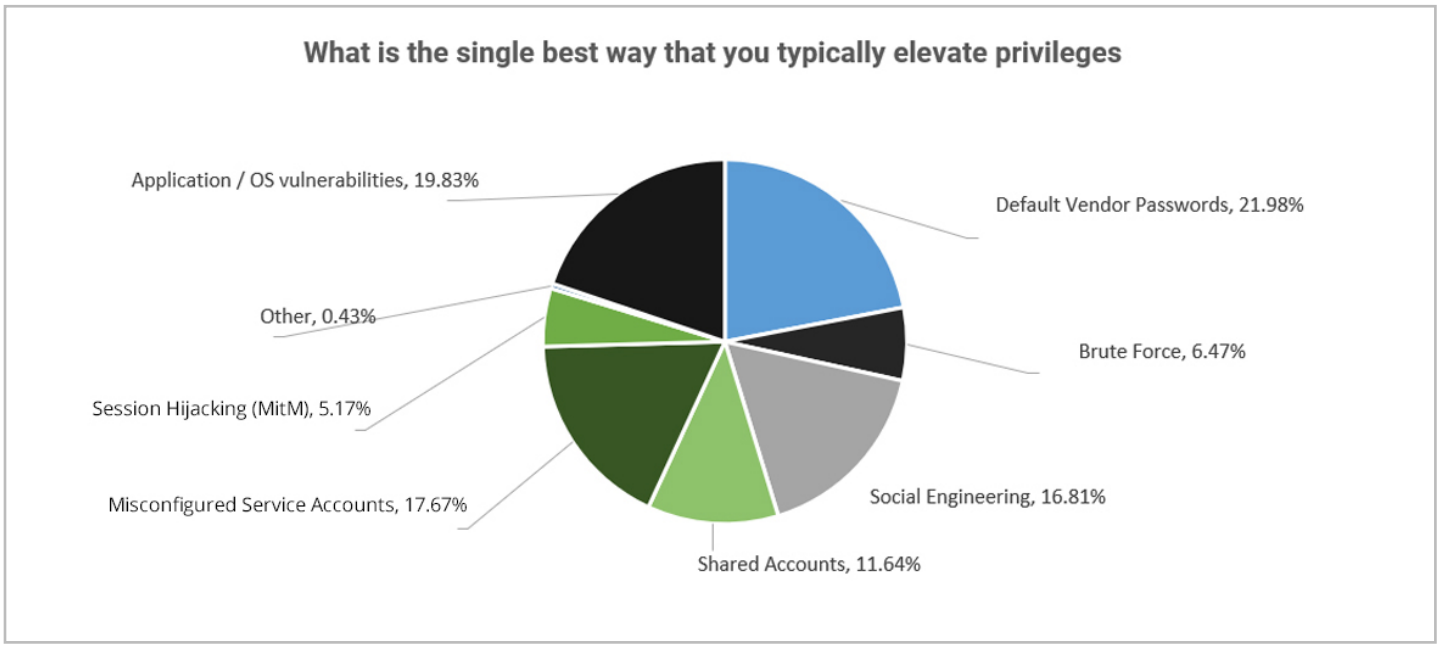
Organizations today focus on getting employees on board and productive as quickly as possible and invest heavily in identity provisioning solutions that help create the accounts employees need to perform their jobs. However, hackers tell us that companies are typically giving users far more access than is necessary, especially for local admin accounts.



Default vendor passwords allow hackers to escalate privileges.

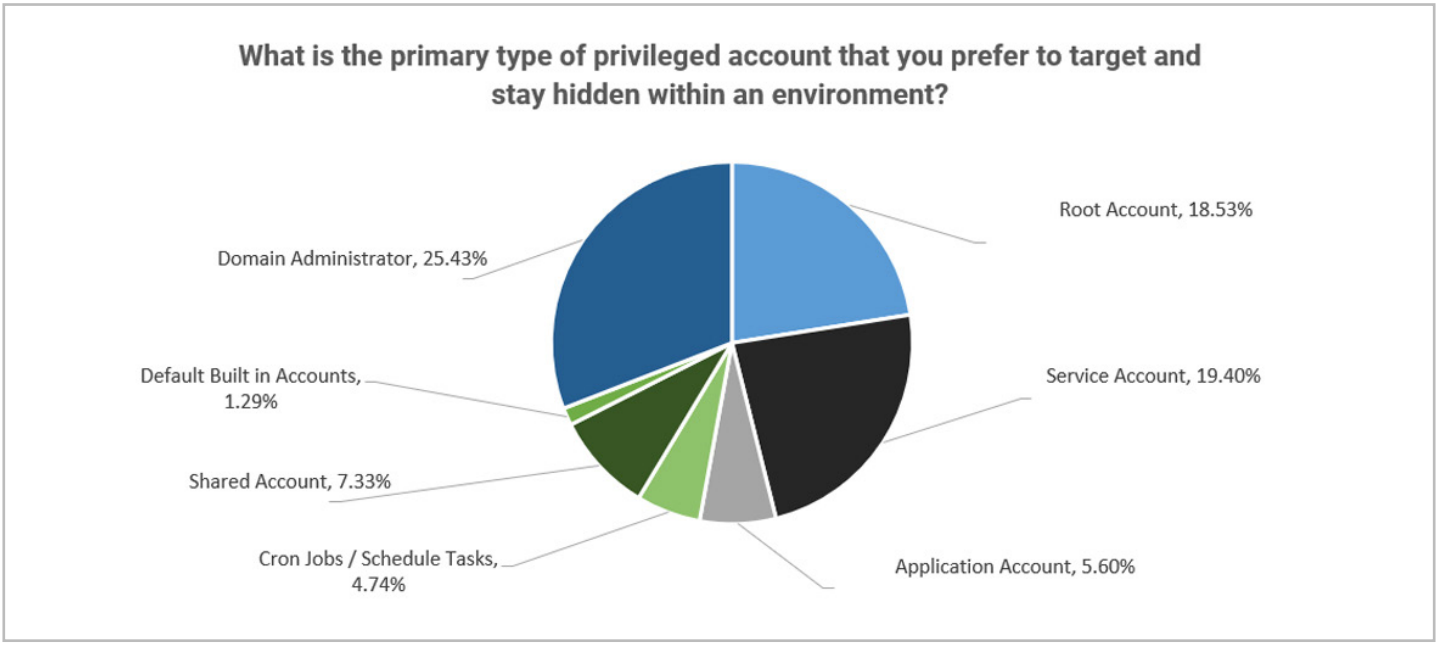
With social engineering as the fastest way onto a network, 22% of hackers confirmed that default credentials continue to be the Achilles heel of organizations. Thus, hackers still find many systems and applications with default credentials, allowing them to easily bypass security controls and get at privileged accounts. Organizations

Exploiting application and OS vulnerabilities was cited by 20% of hackers to elevate privileges once they have gained network access. This research confirms that while patching applications has been a priority for many years, patch management remains a significant and constant challenge



Domain Admin accounts allow hackers to RULE the network

Hackers say the Domain Administrator account is the most desirable account to take over, allowing them to do just about anything they want on the network. Other popular accounts targeted include Service Accounts, Root Account and Local Administrator Accounts---all of which allow an attacker to move around easily, stay hidden, and perform malicious activity.



RECOMMENDATIONS

Organizations need to identify and control Administrator privileges, including local admin accounts that many IT professionals continue to give to employees to help avoid support calls. Least privilege with application control is a technique that allows companies to remove local administrator rights from end-users, using application control to validate trusted applications and elevate only those trusted known applications without the need to give employees admin rights. Organizations need to start implementing the principle of least privilege while balancing productivity, ease of use and security in a dynamic environment.

To successfully implement least privilege, security and desktop teams must work together to create application control policies that match the needs of the organization. Organizations can start by using an automated discovery tool that saves time identifying which endpoints and local users have admin rights, and knowing what applications are in use and if they require admin rights to run. Even when software inventory systems show applications managed and approved by IT, users may have downloaded software or accessed SaaS tools that haven't made it onto the list.

Learn more

Free Endpoint Applications Discovery Tool
thycotic.com/free-endpoint-discovery/

Insider's Guide to Successfully Implementing Least Privilege
thycotic.com/least-privilege-insider-guide

REPORT SUMMARY

The 2018 Black Hat Hacker Report indicates that our operating systems and endpoints remain woefully vulnerable to threats from hackers and cyber criminals. By combining a least privilege strategy with other security layers such as multi-factor authentication, biometrics, behavior analytics and privileged account protection, organizations can build and maintain a more effective and dynamic security posture to keep hackers from exploiting their IT environments.

ABOUT THYCOTIC

The easiest to manage and most readily adopted privilege management solutions are powered by Thycotic. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, D.C., Thycotic operates worldwide with offices in the UK and Australia. For more information, please visit www.thycotic.com

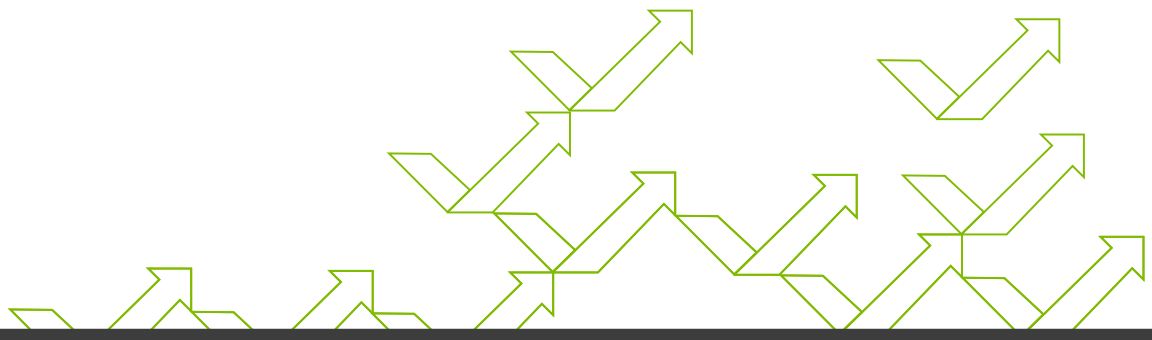
SEE HOW EASY IMPLEMENTING LEAST PRIVILEGE CAN BE

Try Privilege Manager Free for 30 Days

Try Thycotic Privilege Manager free for 30 days. You'll be able to create application control policies, including whitelisting, blacklisting and greylisting, and enforce least privilege without impacting productivity.

START TODAY

thycotic.com/PrivilegeManager/



e: sales@thycotic.com
t: @thycotic
www.thycotic.com