PONEMON 2014 SSH SECURITY VULNERABILITY REPORT

INFORMATION TECHNOLOGY'S DIRTY SECRET AND OPEN BACKDOORS

UNDERWRITTEN BY VENAFI, INC.

KEY FINDINGS

Unprotected SSH cryptographic keys make nearly every enterprise server, virtual machine and cloud service vulnerable to cyber attacks. Key Ponemon research findings include:

- Three out of four enterprises have no security controls for SSH that provides cyber attackers root access
- Over half of enterprises acknowledge that their organizations have already experienced an SSH key-related compromise
- Yet 46% of enterprises do not rotate or change SSH keys, in spite of the fact that SSH keys never expire, which means this represents a perpetual vulnerability

EXECUTIVE SUMMARY

Global organizations are under attack, and the attackers are more dangerous and persistent than ever. Armed with a litany of next-generation cybercrime tools, they're vastly different from yester-year hackers and better enabled with targeted and persistent tools. While the motivations vary, the goal of today's cybercriminal and nation-state attacker is to become and remain trusted on targeted network in order to gain full access to sensitive, regulated and valuable data and intellectual property, and circumvent all existing controls.

Enterprises are increasingly turning to "next-generation" cybersecurity controls to detect advanced attacks, safeguard sensitive data and IP, and reduce the risk of compliance violations and data breaches. While the trend to deploy bigger, better and smarter end user devices and lower-cost, scalable software, and virtualized hardware continues, the basic technology building blocks of network trust remain firmly rooted within virtually all Global 2000 organizations.

Research findings in this report reveal that enterprises are dependent and rely heavily on the Secure Shell cryptographic protocol (SSH) to ensure online trust and to protect valuable information, just as they should. When used correctly, SSH is a solid IT security protocol that keeps an organization's virtual security doors firmly locked and accessible by only the appropriate networked systems and users. Unfortunately, when left unprotected—through lack of visibility and controls—this security technology can be misused by malicious insiders and other cybercriminals, allowing them to authenticate into systems, servers and databases. The use of SSH keys provides adversaries with privileged and root status, which allows unfettered access to systems and data.

The research also found that most respondents have no way to control, account for, or protect the thousands of SSH keys in use within their IT environments. A finding proving that the lessons learned from Edward Snowden's attack on the NSA, where SSH keys provided undetected access that allowed him to steal droves of classified documents, has changed little within Global 2000 organization's policies, procedures or controls for unprotected SSH keys.

SSH AND NEXT-GENERATION VULNERABILITES

Underwritten by Venafi, the Ponemon 2014 SSH Vulnerability Report reveals that SSH key security processes are, at best, weak within Global 2000 organizations. It further demonstrates that the world's most highly targeted enterprises are doing little to nothing to correct critically flawed cybersecurity processes that are leaving SSH keys—and by extension data—exposed.

Among the fundamental security controls the Global 2000 rely on to ensure trust is the secure shell protocol (SSH). SSH clients remotely connect system administrators and automated processes to services, appliances, and cloud services over an authenticated, encryption channel. Everything from payment servers, healthcare databases, cloud platforms, and even air traffic control systems are accessed and controlled by administrators via SSH keys.

System and application administrators, not IT security, are responsible for securing and protecting the SSH estate. This situation exposes critical security vulnerabilities, which are compounded by two facts. Together, these represent IT's dirty little secret, which leave known and open back doors for cyber-criminals to compromise networks[1]. Since SSH-level authentication sessions represent encrypted traffic, they are not typically visible to network monitoring technologies.

Data loss prevention, advanced threat detection solutions and next-generation firewalls cannot consume SSH encrypted traffic, making it easy for adversaries to steal information—over extended periods—without detection. And unlike digital certificates, SSH keys never expire, leaving the vulnerabilities and figurative back doors open indefinably.[2]

Although the findings are alarming, SSH keys themselves are not the problem. The problem arises from the way enterprises deploy, account for and protect them; and the problem is exacerbated by a wide-spread inability to detect anomalous SSH keys and the misuse of existing ones.

Among the most alarming findings revealed by this report:

---

[1] This happened earlier this year when GitHub, the popular web-hosting provider for software developers, exposed software developers SSH private keys via a search function upgrade. As a result cyber-criminals used the exposed SSH keys to launch their own workloads in the cloud—at the expense of the organizations developers worked at—to be used for malicious activity and gain access to the software developers systems. This demonstrates the lack of visibility or control of how application admins secure their SSH keys. For more information see: https://github.com/blog/1390-secrets-in-the-code. http://www.theregister.co.uk/2013/01/25/github_ssh_key_snafu/ and http://www.securityweek.com/github-search-makes-easy-discovery-encryption-keys-passwords-source-code

[2] This vulnerability is not hypothetical. Take, for example the case where an admin leaves an organization, but retains his or her SSH private key and thereby retains access to all the connected systems and applications. This represents an open backdoor because the organization does not have a clear understanding of where the SSH keys are and relies on application admins to self-manage their own keys.

- 51 percent of respondents admitted that their organizations have already been impacted by an SSH key-related compromise in the last 24 months.
- 60 percent of respondents reported that their organizations cannot detect new SSH keys introduced onto their networks; relying on administrators to report and track them manually and without oversight.
- 68 percent of respondents admitted that their organizations have no automated process for SSH key policy enforcement.
- 74 percent allow administrators to independently control and manage SSH keys, which provides would-be hackers unfettered, root access.
- 53 percent of respondents' organizations no not have centralized control over their SSH keys.
- 54 percent of respondents that use home-grown, scripted solutions to detect new SSH keys were still compromised by rogue SSH keys on their networks in the last 24 months.
- 82% of organizations change keys or change them at best every 12 months - while average IT user is changing password every 60-90 days. And SSH keys never expire, which means this represents a perpetual vulnerability.[3]
- 76 percent of enterprises report no systems to secure SSH when using the cloud.

SSH Keys: Open Doors Guarded by No One

The survey also revealed that there are foxes' springing up in global enterprises that are — either on purpose or by accident — gaining charge of the information hen houses. Although SSH keys are an IT security technology, they are often left unchecked in the hands of a wide-range of administrators that are not, in theory or practice, IT security experts. This dirty little secret, revealed by the survey, is further evidence to the fact that root access to the world's most sensitive data is widely available and largely unprotected. In fact, the research found:

- 50 percent of respondents' organizations give network ops, UNIX ops, application administrators and others responsibility for securing SSH keys.
- Only 13 percent of respondents' organizations grant IT security specialists SSH key protection authority.

Tolerated Insanity

The 2014 Ponemon SSH Vulnerability Report revealed alarming statistics and conclusions, including that CEOs, CIOs, CISOs and other IT security executives are tolerant to the point of insanity when it comes to controlling, protecting and detecting the most widely used security and authentication technology in use

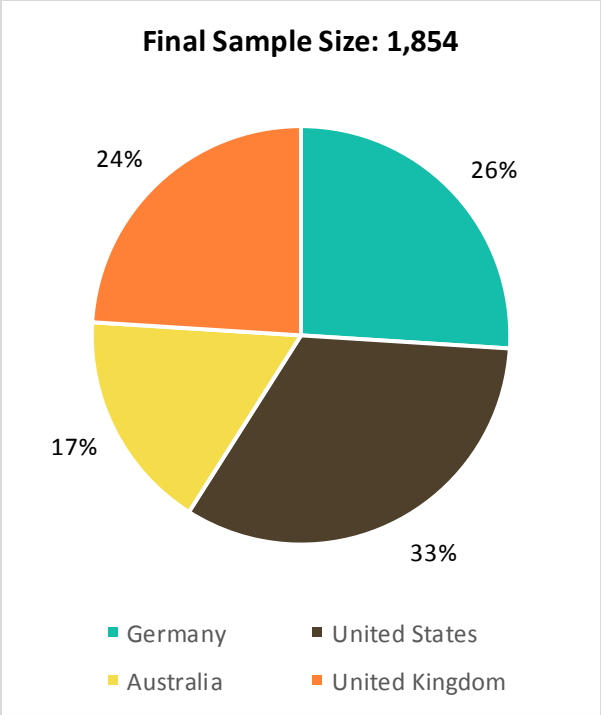
3 There are thousands of malware samples designed to steal keys and certificates for malicious actors to use in their campaigns against organizations. However, what most organizations fail to perform when removing malware is to rotate keys and certificates. Take for example the Mask malware that was recently discovered; it has been in circulation since at least 2007, stealing certificates and SSH keys along with documents and other encryption keys in over 30 countries. The malware is signed with digital certificates and uses SSL for secure communication back to the command and control, while the malicious actors use the stolen SSH keys for remote access to victims machines. More information is available in the full report: http://www.securelist.com/en/downloads/vlpdfs/unveilingthemask_v1.0.pdf

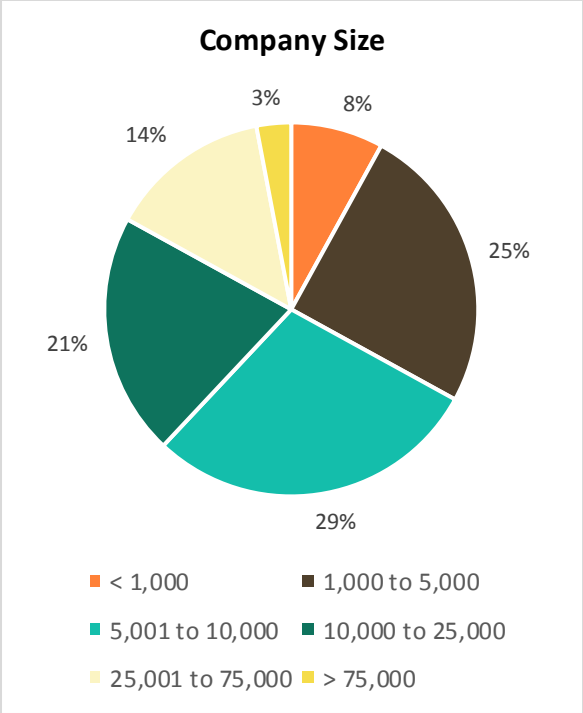
today. They have allowed SSH security to spin out of control, which in fact places their organizations in jeopardy—a situation that is the exact opposite of what they intended to prevent through the use of SSH.

The problem only gets worse as virtualization, software defined networks, and IaaS create hundreds or even thousands of vulnerable servers in a matter of seconds. With no visibility or control, enterprises will pay the price as attackers amp up their exploitation of this vulnerability that gives root access away and doesn't expire.

Demographics

This report included a survey of 2,136 respondents from Global 2000 enterprises in four countries across Australia, Germany, the U.K. and the U.S. More than 50 percent of respondents are employed in companies with 1,000 to 10,000 employees. Conducted during Q1 2014, the demographics breakdown for the survey was:





CONCLUSION

By using a stolen SSH key, an adversary can gain rogue root access to enterprise networks and bypass all the security controls. Because organizations have no policies, visibility into SSH vulnerabilities, or ability to respond to an SSH-related attack, cyber-criminals are turning to SSH as an attack vector at an ever-increasing rate. Every organization needs to stop viewing SSH keys and the management thereof as an operational matter that can be resolved with a few simple discovery scripts or relying on individual application administrators to self-govern. You wouldn't do that with domain credentials, so why treat SSH keys—which enable elevated root privilege—any differently?

Every organization needs to have central visibility into the entire SSH key inventory, understand how SSH keys are used on the enterprise network, and apply SSH policies Only then will an organization be able to quickly detect security incidents related to SSH and immediately remediate them.

An exclusive new infographic is available and provides you with the analysis needed to understand the breach and how it could impact you and your organization. Download now.

About Ponemon Institute

Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

About Venafi

Venafi is the market leading cybersecurity company in Next-Generation Trust Protection (NGTP). Venafi delivered the first trust protection platform to secure cryptographic keys and digital certificates that every business and government depend on for secure communications, commerce, computing, and mobility. As part of an enterprise infrastructure protection strategy, Venafi Director prevents attacks on trust with automated discovery and intelligent policy enforcement, detects and reports on anomalous activity and increased threats, and remediates errors and attacks by automatically replacing keys and certificates. Venafi Threat Center provides research and threat intelligence for trust-based attacks. Venafi customers are among the world's most demanding, security-conscious Global 2000 organizations in financial services, insurance, high tech, telecommunications, aerospace, healthcare and retail. Venafi is backed by top-tier venture capital funds, including Foundation Capital, Pelion Venture Partners and Origin Partners. For more information, visit www.venafi.com