**ANATOMY OF A CYBER SECURITY BREACH AND THE SECOND LAW OF THERMODYNAMICS**

[**ANDREW HAMMOND**](http://blog.ssh.com/author/andrew-hammond)

**APRIL 03, 2018**

[**ENCRYPTION**](http://blog.ssh.com/topic/encryption)

**Introduction**

My mother was washing dishes in the kitchen when the glass window she was looking out shattered in front of her…she was OK but unfortunately my curve ball has never gotten better. The second law of thermodynamics dictates that you can't put together something that has fallen apart. There was no way I could put that shattered glass back together.

The second law of thermodynamics applies to breaches. There is no way to go back once you have been breached. This was evidenced by notable incidents at Equifax, Verizon, and Kmart. In fact, 5 million data records are lost or stolen worldwide every single day, according to the Breach Level Index.

**Cost of Data Breach**

The 2017 Cost of Data Breach Study from the Ponemon Institute, sponsored by IBM, puts the global average cost at $3.6 million, or $141 per data record. The average cost of a data breach in the United States is much higher at $7.3 million. Sometimes the real cost of a breach takes time to develop: Yahoo’s 2013 breach was revealed last October costing $350 million off Verizon’s acquisition payment.

**A Specific Example: GoScanSSH**

GoScanSSH, a new strain of malware that has been targeting Linux-based SSH servers exposed to the Internet since June 2017. The malware attempts to obtain a valid SSH credential through a wordlist attack and attempts to infect the host. Upon successful login new malware is delivered infecting the host and the process is repeated.

“GoScanSSH is another example of bad actors looking to exploit SSH keys which provide the keys to the kingdom, said Andrew Hammond, VP of Business Development, customers need to proactively manage important credentials like SSH keys with a policy framework that rotates crypto and sets time expiration.”

**Threat Summary for GoScanSSH**

This advisory is based on research and written reports from **Edmund Brumaghin, Andrew Williams, and Alain Zidouemba of Cisco’s Tallos Intelligence Group. Brumaghin, Williams, and Zidouemba**performed unique and important research on this topic. SSH is highlighting their research as we feel this is potentially a serious threat vector which the community should be aware of. Please refer to their blog of March 26th: **“Discovered by Forgot About Default Accounts? No Worries, GoScanSSH Didn’t”**

[**https://blog.talosintelligence.com/2018/03/goscanssh-analysis.html**](https://blog.talosintelligence.com/2018/03/goscanssh-analysis.html)

**GoScanSSH Specifics**

* targeting Linux-based SSH servers exposed to the internet
* active since June 2017
* has at least 250 domains
* targets the following usernames to attempt to authenticate to SSH servers:
  + admin
  + guest
  + oracle
  + osmc pi
  + root
  + test
  + ubnt
  + ubuntu
  + user
* determines how powerful the infected system is and obtains a unique identifier
* attempts to obtain valid SSH credential through wordlist attack
* upon successful login new malware is delivered infecting the host and process is repeated
* results are sent to a C2 server accessed via the Tor2Web proxy
* avoids military or government systems
* researchers intend to continue monitoring and tracking the attack and have provided blacklists, IOCs, and domains associated with the malware

**Remediation**

Specifically, SSH recommends the following best practices:

1. Define a controlled provisioning and termination process for SSH keys
2. Discover existing legacy keys
3. Monitor key usage and eliminating the 90% of keys that are never used
4. Eliminating policy-violating keys, such as access from DEV/TEST to production or access from personal accounts to service accounts
5. Utilize monitoring, controlling and auditing of encrypted privileged access and data transfers

SSH recommends customers read the research blog of March 26th from Edmund Brumaghin, Andrew Williams, and Alain Zidouemba of Cisco’s Tallos Intelligence Group: **“Discovered by Forgot About Default Accounts? No Worries, GoScanSSH Didn’t”**

[**https://blog.talosintelligence.com/2018/03/goscanssh-analysis.html**](https://blog.talosintelligence.com/2018/03/goscanssh-analysis.html)

**SSH Background and Macro Threats**

The SSH protocol is the de facto standard for remote system administration and secure file transfers.  One of the features behind the adoption of the protocol is the strong authentication using SSH Keys.

SSH keys provide the same access as user names and passwords. They often grant access to privileged accounts on the operating system level, giving a command line. SSH keys have been overlooked in identity and access management planning, implementation, and audits. Users have been able to create and install keys without oversight and controls. These keys are like passwords and **grant access to resources** - production servers, databases, routers, firewalls, disaster recovery systems, financial data, payment systems, intellectual property, and patient information. This has led to violations of corporate access policies and dangerous backdoors. Most large organizations have accumulated large numbers of SSH keys in their environment.

Organizations are finding enterprise wide deployment issues in Secure Shell (SSH) authentication management, which has suffered from lack of governance for years. Many organizations report:

* Large numbers of SSH keys - even several million - and their use is underestimated
* Have no provisioning and termination processes in place for key based access
* Have no records of who provisioned each key and for what purpose
* Allow their system administrators to self-provision permanent key-based access - without policies, processes, or oversight.

Figure 1: External and Unauthorized SSH Access to Root as determined by SSH Risk Assessment

**Case Study: Large Multinational Bank**

They had five million daily logins using SSH, most of them using SSH keys for automation. We analyzed **500 business applications**, **15,000 servers**, and found **three million SSH keys** that granted access to live production servers.

* Of those,**90% were no longer used**.
* **Root access was granted by 10%**of the keys.
* A compromise of a root account allows the attacker to modify the operating system, steal or subvert any data, or install malicious software on the system.

**Business Risk Factors**

* Business continuity
* Reputation loss
* Risk of major financial losses
* Criminal and civil liability for CEO&CFO under Sarbanes-Oxley
* No control of who can access what
* Hackers and malware utilizing SSH
* Backdoors into intranet
* Data leaks under encryption

**Remediation Specifics**

[NIST IR 7966](https://www.ssh.com/compliance/nist-7966/) is a good starting point for understanding how to manage access using SSH. SSH Communications Security also have our own guidelines that build on the NIST guidance. We wrote most of the NIST guidelines, together with the NIST staff, and have the best subject matter experts in the field. SSH Communications recommends utilization of our onsite workshop including the he SSH Risk Assessment. SSH Risk Assessment is a security assessment service that delivers a detailed analysis of how SSH (Secure Shell) is deployed and used in your network and provides an estimate of your SSH key management problem. Long term, SSH Communications recommends a best practice that discovers, monitors, remediates, and manages [SSH keys](https://www.ssh.com/ssh/key/) for interactive and automated connections both in on premise and cloud-based environments.

More generally, organizations can focus on:

* Implementing a security awareness program
* Equifax made a bad situation a lot worse by delaying disclosure, misdirecting potential victims, and failing to patch known vulnerabilities.
* Follow the NIST’s Cybersecurity Framework
* keep tighter control of your data and be aware of GDPR requirements
* scanning the dark web for threat intelligence

**Threat Advisory Briefing**

SSH will be hosting a webinar April 11th with  Sam Curry, Chief Security Officer at Cybereason, Andrew Hammond and Red Curry of SSH Communications Security, and  Hector Monsegur, former Anonymous Hacker and Director of Assessments at Rhino Security Labs entitled “Anatomy of a Cyber Security Breach: The Hero's Journey” which will cover GoScanSSH and many other threats. You can register at the following link:

[**https://www.brighttalk.com/webinar/anatomy-of-a-cyber-security-breach-the-heros-journey/**](https://www.brighttalk.com/webinar/anatomy-of-a-cyber-security-breach-the-heros-journey/)

We will tell you what the emerging threats are, how to prepare, and how to proactively manage an ongoing breach.

SSH Security is also offering a SSH Key Management Workshop which includes a threat advisory briefing to those organizations that are interested. Please contact SSH at [**andrew.hammond@ssh.com**](mailto:andrew.hammond@ssh.com) or sign up at [**https://info.ssh.com/ssh.com-key-management-workshop**](https://info.ssh.com/ssh.com-key-management-workshop) .