ABT Security Systems Client Bulletin

Your server is secretly mining cryptocurrency. It could happen to you.

According to IBM Managed Security Services (MSS) data, network attacks embedded mining tools with the capability to mine several different crypto coins grew notably over the second and third quarters in 2017, has also continued into 2018 and is most likely driven by the aforementioned rising value of crypto coins and attackers’ interest in profiting off of compromised endpoints.

A real case. It could happen to you.

Recently, ABT Security Systems investigated that one of our clients’ servers was compromised using an automated password testing application on vulnerable accounts with weak passwords. The attacker was able to use the hardware resources of their server for Crypto currency (named Electroneum) mining in order to generate financial gain.

The attacker performed an automated password guessing attack (Brute Force) to identify weak credentials in order to gain unauthorised access to the server. After multiple failed login attempts the attacker was able to gain access to the server using the insecure credentials of a user. The attacker created an automated sequence that performs crypto currency mining activities.

This client used a self-managed in-house server. The abnormal operation of the server was noticed by the client when printing was slow. ABT investigated and took immediate actions to stop the unauthorised intrusions:

- **immediately killed the processes the hacker had installed;**
- **changed all users passwords;**
- **actively blocked connectivity to the Pronto server from all but necessary locations.**

The attacker attempted to cover their tracks by clearing all fingerprints and history. However, the attacker was unable to clear the authentication log history. Fortunately, there is no indication that data was accessed.

ABT Online server has applied multiple levels of detection and prevention of unauthorised intrusions.

- 24x7 server monitoring
- Intrusion Prevention Systems in place
- A Human layer of security practices to Cloud services
- Strict client authentication and authorisation
- ABT online support team to educate clients and prevent unnecessary increases in network attack

Document Terminology

Brute Force

Brute force (also known as brute force cracking) is a trial and error method used to gain access to user accounts and passwords. Automated software is used to generate a large number of consecutive guesses as to the password, PIN or password hash.

Crypto Currency Mining

Crypto currency mining is adding more Crypto currency to the digital currency ecosystem by solving complicated mathematical problems. The mining of Crypto currency is usually rewarded in some monetary manner.

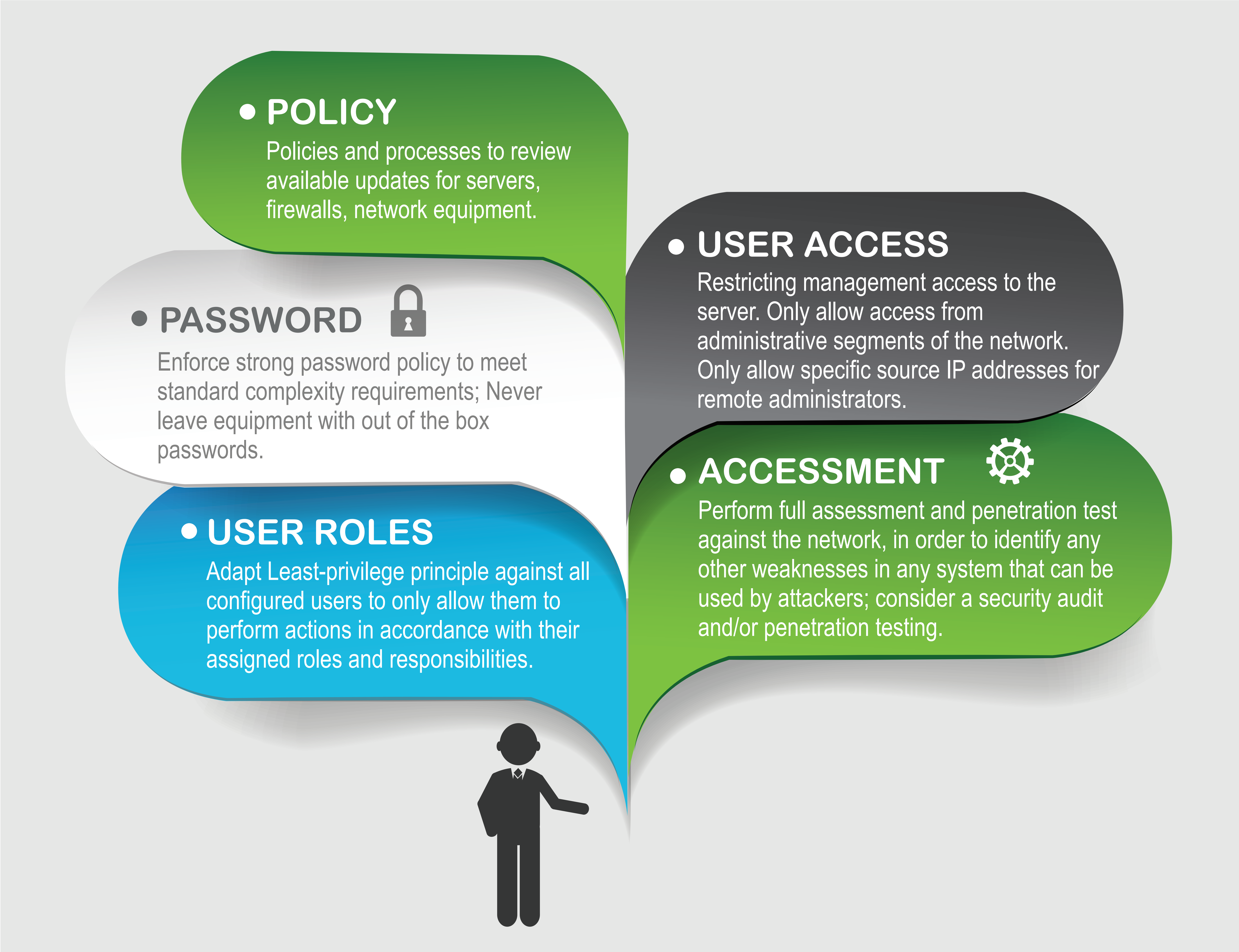
Electroneum

One of many crypto currencies available. Electroneum is a crypto currency aimed at the enhancement of mobile payments.

How to tell if your computer is being used to mine cryptocurrency

The main giveaway is a sudden spike in CPU usage. Most mining scripts try to use as much CPU processing power as possible, so an immediate jump when browsing certain websites or a substantial reduction in processing speed on your server are dead giveaways. Your system may also feel a bit slower when trying to open other windows or programs. You can check the Task Manager on Windows or the Activity Monitor on Macs to check whether usage spikes when you visit a site.

Prevent Unauthorised Intrusions, ABT Security recommend that as a minimum the following steps.



- **POLICY**
  Policies and processes to review available updates for servers, firewalls, network equipment.
- **USER ACCESS**
  Restricting management access to the server. Only allow access from administrative segments of the network. Only allow specific source IP addresses for remote administrators.
- **PASSWORD**
  Enforce strong password policy to meet standard complexity requirements; Never leave equipment with out of the box passwords.
- **ACCESSMENT**
  Perform full assessment and penetration test against the network, in order to identify any other weaknesses in any system that can be used by attackers; consider a security audit and/or penetration testing.
- **USER ROLES**
  Adapt Least-privilege principle against all configured users to only allow them to perform actions in accordance with their assigned roles and responsibilities.

ABT
SECURITY SYSTEMS

A. Level 1, 37 Epping Rd. Macquarie Park NSW
2113 Australia
P. PO Box 363 Macquarie Park, NSW 1670
E. info@abtgroup.com.au
T. +61 2 9878 7111 | F. +61 2 9888 2720
w. www.abtsecuritysystems.com.au

ABT Security Systems stand ready to assist in the implementation of any of the above measures should you need assistance in implementing these controls or security investigation.

Should you wish to further secure your environment ABT Security can provide the security options that can meet your business need. Please do not hesitate to contact:

02 9878 7111