AUSTRALIAN THREAT INTELLIGENCE ANNUAL REPORT 2016-2017

EXECUTIVE SUMMARY

Between January 2016 and July 2017, Mossé Security delivered 53 threat hunting exercises and responded to 67 separate security breaches. We observed 42 Australian firms attempting to deal with cyberattacks and saw firsthand how textbook approaches to information security failed to deter and dissuade attackers.

On one hand, adversaries consistently outsmarted, deceived, frustrated, overwhelmed their victims. And on the other hand, victims almost always failed to anticipate cyberattacks, understand the adversaries' mindset and tradecraft, and fight-back. That is, until they called us and followed our recommendations (we have an emergency number to receive help when a breach is detected: 1300 730 035).

The key points from our report are:

1. 52 out of 53 organisations that engaged us to deliver threat hunting exercises had high-fidelity indicators of compromise on their networks;
2. 7 out of 10 customers were targeted by financially-motivated adversaries with professional hacking and social engineering skills. Most of them paid the ransom, or the extortion fees, or the fake invoice, at least once;
3. Most organisations were breached multiple times by the same adversaries who later decided to come back for more money.

With this report, our company hopes to shed some light on the state of cyber security in Australia, the adversaries, and their tradecraft. We also offer some recommendations on the last page of the report. Call us with any questions you may have.

Key Findings:

52 Out of 53	**Organisations Compromised** Out of 53 threat hunting exercises delivered, only a single company did not have high-fidelity indicators of compromise of its network.
6 Months	**Detection Time** The average time between the first forensics artefact generated by the adversaries and customers detecting the intrusions was 6 months. The main alert triggers were threat hunting and fraud.
18 Months	**Root Cause Remediation** Technical causes of security intrusions were generally remediated in less than 20 days, but the root causes of security breaches took customers over a year and a half to address.
9 Out of 10	**Financially Motivated** Nine out of ten major cyberattacks were linked financially motivated criminals that use IT vulnerabilities to commit fraud, blackmail, ransom and/or extort organisations.

Contact Us:

- Phone: **+61 1300 730 035**
- Web: www.mosse-security.com
- Email: contact@mosse-security.com

MOSSÉ SECURITY
THREAT MATTERS

ADVERSARY PROFILES

Mossé Security categorised the threat actors it observed between January 2016 and July 2017 into four main groups:

	Amateurs	Professionals	Experts	Nation State
Size	1-5 adversaries	3-15 adversaries	+10 adversaries	+100 adversaries
Attacks	SMEs	SMEs	Any organisation	Any organization
Motivations	Financial	Financial	Financial	Political / Military
Approach	High volume, very low returns	Semi-targeted and opportunistic	Targeted, high returns	Targeted
Skill Level	Low	Moderate	High	Moderate to Astonishing
Strategy	Uses basic scare and deception tactics	Overwhelms victims or uses more advanced deception tactics	Completely compromises and deceives their victims	Maintain persistent access into all critical infrastructure
Cost to Victims *	Less than $1K per victim	$30-150K per victim	$500K-3M per victim	Not quantifiable
Example	• Mass email campaigns asking companies to pay fake invoices • Threatens to deliver a DDoS attack unless a small “protection” fee is paid	• Excellent timing of ransomware attacks against companies not equipped with backup solutions • Social engineering capable to trick well-aware people	• Steals gigabytes-worth of corporate and customer data, and threatens to publish it on the Internet unless a high fee is paid	• Long-term compromise campaigns against government agencies, energy and defence firms and financial institutions
Tools	• Basic social engineering	• Good social engineering • Ransomwares and backdoors • Denial of service	• Astonishing social engineering • Custom backdoors • Distributed denial-of-service	• Rootkits and backdoors • Hardware implants • Zero-days
Frequency & Success	All customers targeted. 5 paid	7 out of 10 customers targeted. Majority paid at least once	4 customers targeted. 1 paid	2 customers targeted

(*) Monetary figures quoted don't include cost of brand damage, systems and hardware repairs and upgrades, loss of worked hours, lawsuits etc.

ADVERSARY TRADECRAFT

The following table presents the strategies and tactics adversaries employ to defeat the most common security protections:

Most Common Security Control		Attacker's Strategy & Tactics	Defence Opportunity
Antivirus Software	Easy to Defeat	• Never user known malware and viruses • Memory-only attacks • File protection (e.g. encoding, encryption, packing etc.) • Reliance on existing OS utilities	• Rely on Windows's default antivirus solution (Defender) • Augment AV with application whitelisting and endpoint monitoring • Automate binary and script analysis for executables never seen before in the environment
Firewall		• Attack the endpoints and the web applications • Packet encoding and encryption	• Do not overspend on firewalls. Allocate funding elsewhere
Network Intrusion Detection/Prevention Software		• Domain fronting • Network encoding and encryption	• Rely on the endpoint's antivirus to prevent network attacks • Using statistical analysis, hunt for C2 that uses domain fronting
Strong Passwords		• Steal and replay password hashes • Offline password cracking	• Enforce two-factor authentication whenever possible • Detect password dumping activities
Application Whitelisting		• Use whitelisted Windows executables for offensive purposes • Rely on Windows's scripting capabilities	• Use AppLocker or Windows 10 Device Guard to reduce cost • Hunt for well-known application whitelisting bypasses
Patching		• Exploit human vulnerabilities, not software vulnerabilities • Steal and reuse credentials	• Use Windows 10 Credential Guard • Expect and hunt for spear phishing attempts

Endpoint Detection & Response	Moderate	• Generate low-fidelity indicators of attacks by blending in and "living off the land"
		• Attack endpoints not monitored by EDRs, compromise credentials, and then move laterally like a normal user
			• Combine security monitoring with deception tactics
			  ○ Honey-tokens
			  ○ Honey-credentials

RECOMMENDATIONS

Mossé Security recommends that organisations consider the following recommendations:

Recommendation 1: Get A Realistic View of Where You Stand and Act Pre-Emptively

Companies in this report are bearing the significant costs of inaction. Cyber risk is very real and very present. Nobody is out of danger, or out of reach. Nearly all companies without exception have an unrealistic view of where they stand security wise.

We urgently request that you act now before it's too late.

Having a reactive policy is a lot costlier than a proactive policy. Mossé Security is a trusted third-party provider to help you have an uncomplacent view of your exposure to cyber security risks.

Recommendation 2: Obtain the Right Mental Models to Properly Think About Cyber Security

Most security solutions fail because decision makers do not properly think about IT security. Stopping cyber threats require solutions that blend psychology, technology, processes, economics, legal, intelligence, and criminality. And whilst decision makers do not need to be experts in all these fields, they need to know how to acquire well researched information in all of them to deal with ongoing cyber security issues.

Only after the right mental models have been acquired by decision makers can successful solutions to protect organisations emerge.

Recommendation 3: Employ Structured Analytic Techniques to Manage Cyber Risks

Structured analytic techniques (SATs) are processes and tools meant to mitigate the impact of one's cognitive limitations and pitfalls, improve decision making, solve problems faster and better, generate consensus, and communicate ideas more effectively.

It is imperative that security professionals use SATs when designing security solutions. Otherwise, people just do what they've always done, whether it partially works or not at all.

Examples of SATs include: Red Team vs. Blue Team, Playing the Devil's Advocate, Futures Thinking, Seeing the Other's Point of View, and Kepner and Fourie.

Recommendation 4: Assign Security Compliance Activities to The Compliance Manager

Security compliance is not real security, and yet, the majority of a Chief Information Security Officer's (CISO) or Head of Information Security's role and resources are dedicated to compliance challenges. As a result, organisations are spending more time and resources trying to defend against auditors than cyber attackers.

If you want to drastically improve your cyber security defences, assign security compliance activities to your Compliance Manager and let your CISO focus on protecting your organisation against the attackers you're facing.

ABOUT US

Mossé Security provides world-class cyber security solutions and strategic security advice to government, private sector clients, and security minded individuals.

We operate around the world and our head office is located in Melbourne, Australia.

Contact Us:

Phone: +61 1300 730 035

Web: www.mosse-security.com

Email: contact@mosse-security.com

MOSSÉ SECURITY
THREAT MATTERS