Threat Landscape Update
Internet Security Threat Report (ISTR) 2019
volume 24
https://go.symantec.com/istr

IETF 104, Monday 25th of March 2019, Prague
Arnaud Taddei (Arnaud_Taddei@symantec.com)
Candid Wueest (Candid_Wueest@symantec.com)
Cybercrime Trends – Focused on Profit

FormJacking

• Formjacking is the use of malicious JavaScript to transparently steal payment card information & PII from compromised websites

• On average 4,800 websites were compromised by formjacking attacks every month in 2018

• We blocked 3.7M formjacking attacks in 2018 on endpoint devices

• Difficult to detect for end-users

CryptoJacking

• Cryptojacking activity remains at high levels with 3.5 million blocked events in Dec 2018

• Over the course of 2018, total cryptojacking events dropped by 52% as cryptocurrency prices dropped by almost 90%

• Overall web attacks are up by 56%

• 1 in 10 URLs was malicious (1 in 16 in 2017)
Cybercrime Trends – Focused on Profit

**Ransomware**

- Enterprise ransomware infections are up 12%
- Mobile ransomware infections are up 33%
- Overall ransomware infections were down by 20% as attackers moved to more lucrative activities

**Smartphones**

- 1 in 36 mobile devices had a high risk app installed
- Only 23.7% of Android phones run the latest major OS version. On IPhones 78.3% are on the newest major release
- Social media increasingly used to spread fake news/propaganda
Attack Trends IoT and Cloud

Internet of Things

- 75% of compromised devices were routers, followed by cameras 15%
- 5G connectivity will change the landscape with more directly connected devices
- Weak passwords & device exploits are most common attack vectors
- Used for DDoS, crypto jacking, ad-fraud, but other methods grow

Cloud Environment

- Attacks against AWS, Azure, Kubernetes, Docker, serverless applications and exposed API services increased
- At least 70 million records leaked from AWS S3 buckets in 2018 -> more data breaches
- Vulnerabilities in hardware chips & infrastructure place cloud services at risk: Meltdown, Spectre, RunC, SDN exploits
Targeted Attacks

• Remain undetected for as long as possible, move lateral to many systems
• Spear-phishing remains the primary vector for targeted attacks with 65%
• Intelligence gathering is primary motive (96%)
• APT groups are going after ICS/IoT devices
• Less zero day vulnerabilities used

Living off the Land and Supply Chain Attacks

• The misuse of legitimate system tools a.k.a. “Living off the Land” increased again in popularity - Simple, but effective
• Use of malicious PowerShell scripts increased by 1000%
• Office files accounted for 48% of malicious email attachments, up from 5% in 2017 – Supply Chain attacks up by 78% in 2018
QUESTIONS?

THANK YOU

ISTR: https://go.symantec.com/istr