FireEye
SECURITY REIMAGINED

SPECIAL REPORT

REGIONAL ADVANCED THREAT REPORT:

Latin America 1H 2015

SECURITY
REIMAGINED

INTRODUCTION

We appreciate the opportunity to provide you with unique insight into Latin America's threat landscape for the first half of 2015. For years we have been stating that over 96% of businesses unknowingly host compromised PCs within their corporate networks, and that has not changed. During our assessment, we identified all types of threat actors compromising our customers' networks, including suspected nation state-backed actors looking to conduct cyber espionage, cybercriminals, and hacktivists looking to make a statement.

EXECUTIVE SUMMARY

This FireEye Advanced Threat Report for Latin America provides an overview of the advanced attacks that FireEye detected targeting computer networks in Brazil, Peru, Chile, Mexico, and Argentina in the first half of 2015.

Since the start of the year, FireEye has seen a significant increase in the number of attacks across the Latin American region. As we reported earlier this year, 96% of global organizations are unknowingly breached as threat actors of all kinds increasingly evade traditional security products. This report summarizes data gleaned from the FireEye Dynamic Threat Intelligence (DTI) cloud.

Disclaimer: This report only covers computer network activity of targeted FireEye customers who share their metrics with FireEye. It is by no means an authoritative source for all APT activity targeting Latin America or elsewhere. In this dataset, we take reasonable precautions to filter out "test" network traffic as well as traffic indicative of manual intelligence sharing among our customer base within various closed security communities. We realize that some popular APT tools, techniques and procedures (TTPs) can be reused and re purposed by many different threat actors. To address this issue, we employ conservative filters and crosschecks to reduce the likelihood of misidentification.

DEFINITIONS

Advanced Persistent Threat (APT): Advanced Persistent Threat actors receive direction and support from a national government. Whether their mission is to steal information or cause disruption or destruction, they pursue their objectives tenaciously using a wide range of tools and tactics.

Callback: an unauthorized communication between a compromised victim computer and its command-and-control (CnC) infrastructure.

Remote Access Tool (RAT): software that allows a computer user (for the purposes of this report, a threat actor) to control a remote system as though he or she had physical access to that system. RATs offer numerous features such as screen capture, file exfiltration, etc. Typically, an attacker installs the RAT on a target system via some other means such as spear phishing or exploiting a zero-day vulnerability, and the RAT then attempts to hide from the system's legitimate owner.

Security Event: FireEye regularly discovers a wide variety of web, email and file-based threats, including the opening of a malware attachment, a click on a malicious hyperlink, or the callback of an infected machine to its CnC network.

Targeted attack: a unique, malicious event conducted between an APT threat actor and a specific victim network.

Threat Actor: the perpetrator behind cyber activity. This actor could be part of a broader group such as a military unit, an intelligence agency, a contractor organization or a non-state actor with indirect state sponsorship.

Tools, Techniques, and Procedures (TTPs): the characteristics specific to a threat actor's actions and tools (like malware) employed against a victim network. APT actors normally employ multiple TTPs, and multiple APT actors can also use the same TTPs. This dynamic frequently complicates cyber defense analysis.

Vertical: one of FireEye's distinct industry categories: Aerospace, Chemicals, Construction, E-Commerce, Education, Energy, Media/Entertainment, Finance, Government, Healthcare, High-Tech, Insurance, Legal, Manufacturing, Other, Retail, Services, Telecom, Transportation and Wholesalers.

Target: the recipient of a threat actor's attack. In most cases, the low "false positive" rates inherent in FireEye alerts suggest that the discovered attack was successful.

Brazil continues to be the most targeted country in Latin America

Cyber Threats to Latin American Countries

Top five target countries with alerts on malicious exploits/downloads:

1. Brazil
2. Chile
3. Mexico
4. Peru
5. Argentina

Brazil continues to be the most targeted country in Latin America, followed by Chile and Mexico. Cyber crime continues to pose a threat to individuals and organizations in Latin America as the population becomes increasingly internet-connected, and as online banking and payment systems become more widespread.

Top five countries exhibiting CnC infection callbacks:

1. Brazil
2. Peru
3. Mexico
4. Chile
5. Argentina

The most compromised countries with the highest number of "successful attacks" were Brazil, Peru and Mexico despite Chile being more heavily targeted than Peru. This discrepancy highlights that being more targeted does not directly lead to more successful compromises and that Chile's security practices could be more effective than its peers.

Top 10 industries with alerts on malicious exploits/downloads:

1. Financial Services
2. Chemicals/Manufacturing/Mining
3. CPG(Consumer Products Group)/Retail
4. Energy/Utilities
5. Services/Consulting
6. Government: Federal
7. Healthcare/Pharmaceuticals
8. Telecom
9. Aerospace/Defense Contractor
10. Insurance

Top 10 industries exhibiting infection callbacks:

1. Chemicals/Manufacturing/Mining
2. Financial Services
3. Energy/Utilities
4. Government: Federal
5. CPG(Consumer Products Group)/Retail
6. Healthcare/Pharmaceuticals
7. Services/Consulting
8. Telecom
9. Aerospace/Defense Contractor
10. Entertainment/Media/Hospitality

The chemicals/manufacturing/mining industry in Latin America continues to be most impacted by attacks. Interestingly, attacks against private sector or non-governmental organizations – e.g.,Financial Services, Energy/Utilities, and CPG – have displaced federal, state, and local governments as the most targeted industries in the region. Despite the slowdown in the Latin America economy, we believe this indicates the rising value of Latin America businesses to threat actors.

Top 10 “destination” countries for CnC callbacks:

1. USA
2. Russia
3. Netherlands
4. Germany
5. Brazil
6. Canada
7. Ukraine
8. France
9. United Kingdom
10. China

It’s interesting to note that, based on the amount of command and control communications, Brazil, the USA, and Russia are among the top nations Latin American organizations see their compromised machines connect with. While these communications provide a look at where attackers are hosting their communication infrastructure, it does not necessarily indicate the attackers are based in those countries.

Top 10 signature families by infection callback count:

1. Trojan.Kelihos
2. Malicious.URL
3. DTI.Callback
4. Backdoor.Kelihos.F
5. Malware.ZerodayCallback
6. Backoor.H-worm
7. Trojan.Necurs
8. Trojan.Rerdom.A
9. Local.Infection
10. Trojan.CryptoWall

The appearance of Trojan.CryptoWall is unique among the common malware families not associated with APT actors. CryptoWall, a ransomware that is fairly easy to detect, is not normally seen with high impact globally. Its prevalence in Latin America shows that threat actors are finding more than enough effectiveness in this common piece of ransomware to continue using it for their own benefits.

Top five APT malware families by infection callback count:

1. Backdoor.APT.Kaba
2. Backdoor.APT.Spynet
3. Backdoor.APT.LV
4. Backdoor.APT.Gh0stRAT
5. Backdoor.APT.XtremeRAT

CONCLUSION AND RECOMMENDATIONS

This report demonstrates that organizations in the Latin America region were increasingly targeted by advanced threats in the first half of 2015. However, while the top malware used to target these countries is not unique to the Latin America region, their use against other high-value nations in other regions indicates the growing value of the data in Latin American corporations and governments.

Our recommendations include:

1. Ensure existing security tools are up to date. Much commodity malware can be easily addressed with legacy, signature-based tools.

2. Implement an Adaptive Defense security model that can help shorten the time it takes between finding a breach and stopping it.

3. Develop new ways to collaborate with other corporations, trade groups, and governments to share threat intelligence.

To learn more about
how FireEye can help you focus
on the alerts that matter,

visit:
http://www.**fireeye.com**

FireEye

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**