eSENTIRE

DATA SHEET:
Inside the Mind of a Hacker

Personal data as a key for intrusion.

A hacker does not necessarily need to be an expert in malware or PowerShell commands to make an attack successful. Oftentimes, Open Source Intelligence (OSINT), a fundamental and simple technique, makes the biggest difference.

We live in a world where people constantly share personal information online. This dynamic gives threat actors endless opportunity and time to use personal data as a key that allows easy entry into a target's network. This real eSentire Red Team engagement gives an up close look inside the mind of a hacker. Identifying details from the engagement have been omitted for confidentiality.

WHAT IS RED TEAM TESTING?

This scenario is an authorized, nearly no-holds-barred simulation of an advanced and stealthy threat actor. Red Team engagements are designed to test an organization's prevention, detection and response abilities over a longer period of time than more traditional forms of penetration testing.

STEP 1 - INFRASTRUCTURE SCANNING

- Scanned the target's infrastructure to discover any exposed applications or servers that could be exploited
- A password reset application was discovered and identified as a possible vector for intrusion
- Four pieces of personal data were required to reset the password: user name, date of birth, social security number and place of birth

of organizations feel they lack visibility on in-use web applications

-Tenable/Cybersecurity Insiders 2018

STEP 2 - IDENTIFY A TARGET USER AND THEIR USERNAME

- Identified a user within the target organization as the subject to hack the password reset tool
- A user with a unique first and last name was targeted for easier identification in the OSINT process
- Free online scraping tools easily confirmed the target's username

50+

free scraping tools with four-star ratings or higher available on Google Chrome's app store, as of June 2019

STEP 3 - DISCOVER DATE OF BIRTH

- Social media profiles, legitimate “find a person” websites and data dumps from breaches were leveraged to verify the target user’s date of birth

7,859,520,210

compromised accounts tracked by leading open-source data breach aggregator

- Tenable/Cybersecurity Insiders 2018

STEP 4 - DISCOVER SOCIAL SECURITY NUMBER

- Social security numbers are widely available for purchase on the Dark Web

$1

Cost of a Social Security number

$30

Cost of a “Fullz” stack of data that includes social security number, date of birth, address and account information

STEP 5 - DISCOVER PLACE OF BIRTH

- Place of birth is not as common of a data type used online, making it more difficult to discover
- Fake social media accounts were leveraged to friend and connect with the target user on multiple platforms
- In the absence of more concrete data, monitoring of the target user’s social media accounts offered clues, and cross-referencing old photos, connections, events attended and support of a local school pointed toward a place of birth

observed success rate of Facebook phishing lures

- eSentire 2018 Threat Report

THE RESULT

eSentire’s Red Team successfully hacked the exposed password reset tool. Once inside the network, the team was eventually able to compromise 39 other accounts, including an account with IT administrative privileges. Ultimately, eSentire’s Red Team gained access to the following:

- Corporate credit card number
- Documents on fiscal year planning and strategy
- Confidential price list on products and services
- Information on existing customers

THE TAKEAWAY

Hackers have the time and resources to perform the necessary reconnaissance that makes a targeted attack successful.

Organizations can take preventative measures, such as training employees to take extra precaution in their personal and professional online activities. However, this only goes so far to mitigate the inevitable risk of human error.

Protection from a targeted attack requires swift detection and response capabilities. A Security Operations Center (SOC) has the necessary combination of people, process and technology. For organizations who lack the expertise or budget necessary to build an internal SOC, Managed Detection and Response services are a viable alternative.

eSENTIRE®

eSentire, the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire.**