Inside the Keysight Security Report 2021

Media Abstract	***04.21.2021***
Beth Hespe, Keysight Technologies	

The Keysight Security Report

The fourth edition of this Keysight Technologies Security Report continues work from Ixia, acquired by Keysight in 2018.

This report combines lessons learned in 2020 with impactful predictions for 2021.

Both the data and the predictions are based upon research conducted by Keysight's Application and Threat Intelligence (ATI) Research Center.

WHITE PAPER

Keysight Technologies 2021
Security Report

Introduction

Welcome to the fourth edition of this Security Report issued by Keysight Technologies, and formerly Ixia. This report combines lessons learned in 2020 with impactful predictions for 2021. Both the data and the predictions are based upon research conducted by Keysight's Application and Threat Intelligence (ATI) Research Center.

The purpose of this report is to help strengthen global cybersecurity. Effective cybersecurity needs to be a collaborative function by security experts. This report is one way of sharing what Keysight has learned over the past year with the international community of security practitioners. We hope it will help security teams think about their security architecture vulnerabilities and how they can better prepare for future attacks.

There were three trends that characterized cybercrime for most of 2020:

- Cybercrime did not take a holiday during the pandemic. Keysight research shows that there was a 62% increase in phishing attacks in 2020 over 2019. In fact, we saw a rapid increase as the pandemic took center stage in March and April.
- Monetary gain took center stage as a key cybercrime motivator. There was a huge uptick in the deployment of ransomware starting in June. While this trend was directed across all industries, healthcare was hit especially hard. The second half of 2020 was particularly brutal with 59% of the attacks occurring during that timeframe.
- Supply chain attacks hit the headlines with the SolarWinds attack. The supply chain continues to be a weakness since the infamous Target point of sale breach in 2013 brought this type of risk to the forefront. The SolarWinds attack reinforces the need for security architects to embrace a holistic and comprehensive approach.

In this report, we'll look into three core attack vectors used in 2020 along with what you need to know to thwart those attacks. The last section discusses the main relevant threats we see for 2021.

Monetary gain took center stage as a key cybercrime motivator. There was a huge uptick in the deployment of ransomware starting in June with 59% of attacks occurring in the 2nd half of 2020. While this trend was directed across all industries, healthcare was hit especially hard.

KEYSIGHT TECHNOLOGIES

Find us at www.keysight.com

Page 1

Three Key Trends

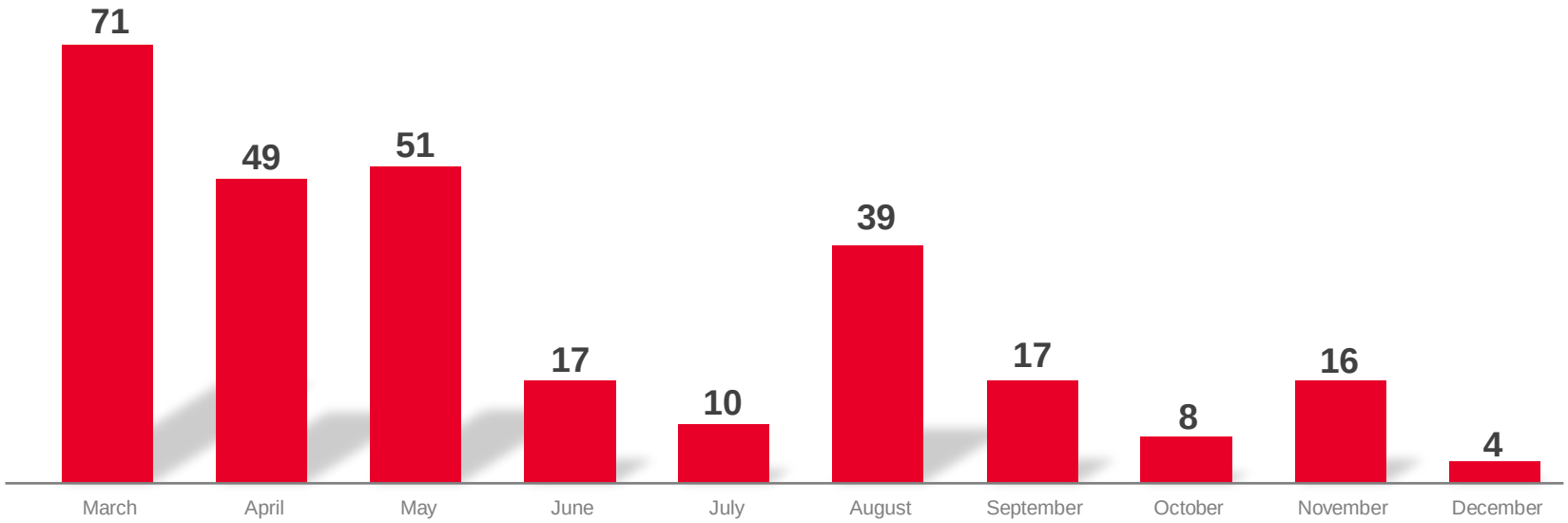
THREE TRENDS CHARACTERIZED CYBERCRIME FOR MOST OF 2020

- **Phishing attacks increased by 62 percent.** Keysight research shows that there was a 62 percent increase in phishing attacks in 2020 over 2019. In fact, there was rapid increase in these attacks as the pandemic took center stage in March and April as social engineering attacks were related to the pandemic.
- **Monetary gain took center stage as a key cybercrime motivator**. There was a huge uptick in the deployment of ransomware starting in June. While this trend was directed across all industries, healthcare was hit especially hard. 59 percent of the attacks occurred during the second half of 2020.
- **Supply chain attacks hit the headlines with the SolarWinds attack**. The supply chain continues to be a weakness and the SolarWinds attack reinforced the need for security architects to embrace a holistic and comprehensive approach.

Trend 1 – Phishing Attempts Targeted The Pandemic

- 62% increase in phishing attacks in 2020 over 2019
- People trying to get financial, or healthcare assistance were prime targets for COVID-19 phishing campaigns

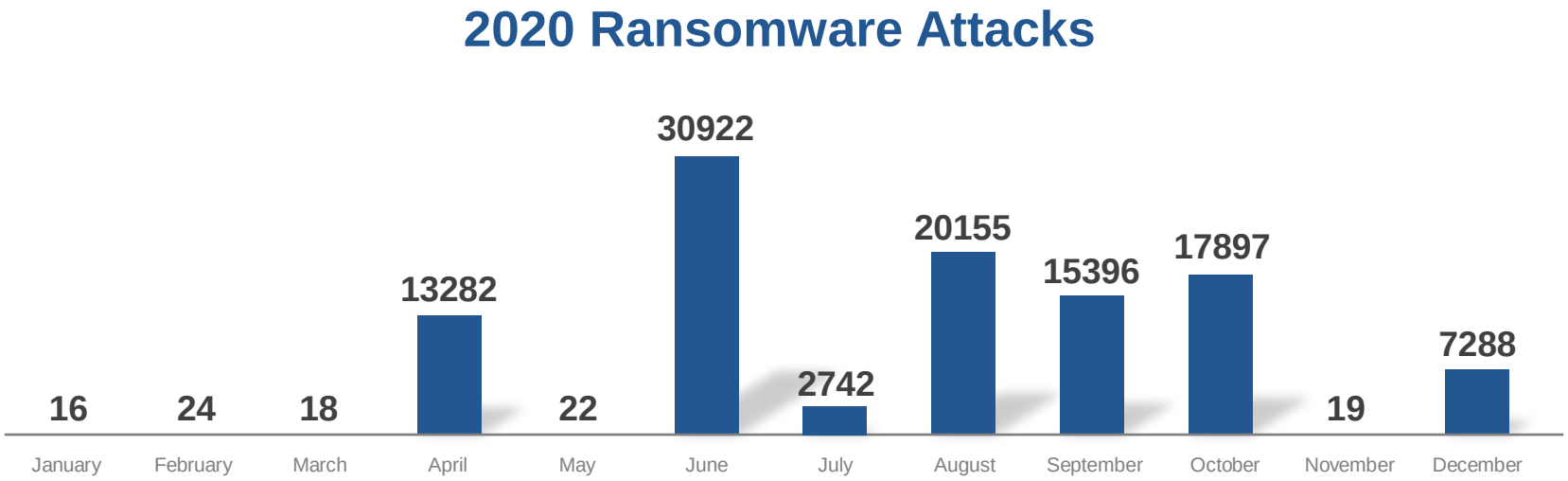
"COVID-19" Phishing Scams Identified by Keysight ATI Rapsheet



Strategic Insight: Phishing and additional social engineering attacks will continue to take advantage of pandemic-related headlines. Keysight's recommendation: End user education is a must. Train users to avoid clicking on links in emails and text messages and go directly to a trusted healthcare site and find the registration link.

Trend 2 – Ransomware Attacks Surged for Healthcare

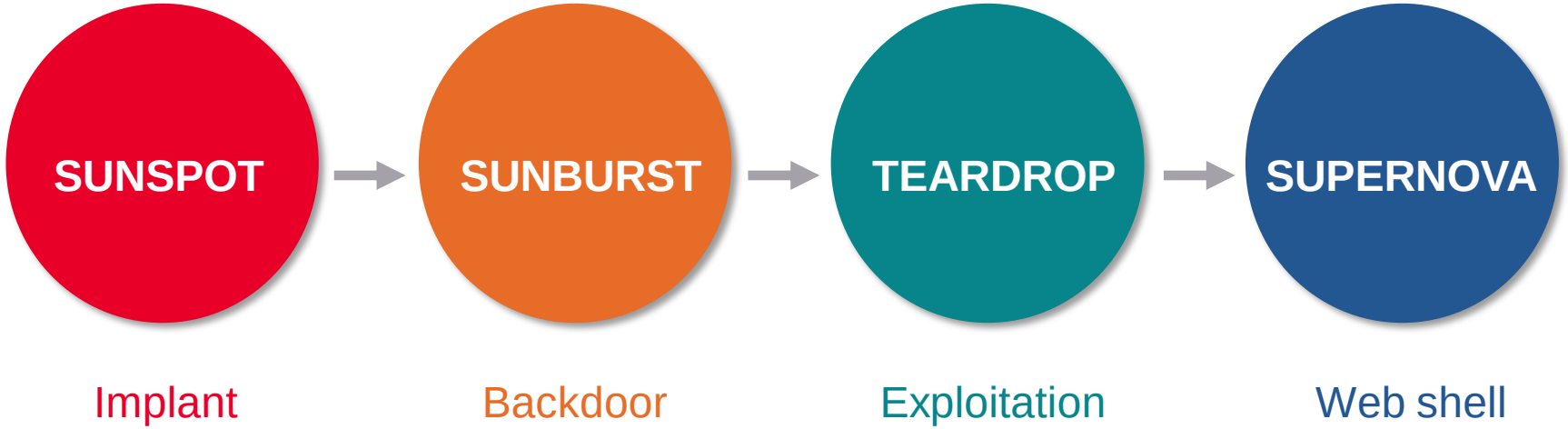
- 59% of all ransomware attacks occurred during the 2nd half of 2020
- While some bad actors claimed they would not target healthcare facilities, many did



Strategic Insight: Ransomware is highly popular because it makes a lot of money for bad actors. Business models continue to mutate along with malware variants. Keysight's recommendation: It's critical to keep enterprise threat detection systems up-to-date with the latest signatures and behavioral patterns, as ransomware builders are getting better at obfuscation and avoiding detection. In addition, network security teams should also be aware that exploitation practices evolve.

Trend 3 – SolarWinds: The Most Effective Supply Chain Attack to Date

- 18,000 SolarWinds customers impacted
- A new model of attacks – malware components nested within other attacks



Strategic Insight: An organization's supply chain is more than just components. There is a tendency to think of a supply chain as outside entities that either supply a company with software and hardware components or the supplies used when building a product. Keysight's recommendation: The supply chain is critical to the operation of a business, including utilities, email, cloud providers, and even coffee suppliers. Network security must consider non-traditional components that may touch an organization and IT systems.

What to Watch For in 2021

- This report concludes with the following key take-aways:
  - Act like your network has already been compromised
  - Create a plan to quantify risk and impact
  - Assess and validate your current operations
- What should you be doing right now? Look for any indicators of compromise
- Do you have everything you need to perform that investigation?
  - Create a data collection infrastructure — taps & packet brokers
  - Insert appropriate security tools — DLP, IDS, and DPI solutions
  - Quantify risk and impact to prioritize tasks
  - Continually assess and validate your operations with BAS solutions