KEYSIGHT

Security Report 2023

March 2023

EXCERPT - Keysight's View of 2023 Threats

Table of Contents

Introduction 3

2022 – A Year in Review 3

CISA Alerts for Vulnerabilities in 2022 10

Android Malware with Focus on Polymorphism 18

Keysight's View of 2023 Threats 27

Conclusion 29

Appendix A – MITRE ATT&CK Review 32

Introduction

Welcome to the fifth edition of this security report issued by Keysight Technologies, and formerly Ixia. This report combines lessons learned in 2022 along with predictions for 2023. 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 2022:

- Malware as a service became more prevalent
- Ransomware continued in full force with attacks on healthcare leading the way[1]
- Threat actors continue to leverage old vulnerabilities in campaigns

In this report, we will explore these three trends from the perspective of our research data along with published MITRE Corporation information. We then suggest three areas of focus for enterprises in 2023 to help protect themselves.

Specifically, this report will cover the following areas:

- 2022 – A year in review
- CISA alerts for vulnerabilities in 2022
- Android malware with focus on polymorphism
- Top vulnerabilities disclosed in 2022
- Our view of potential 2023 threats
- Some suggestions for actions that can be taken

1 Mathew J. Schwartz, "Healthcare Most Hit by Ransomware Last Year, FBI Finds," Data Breach Today, February 27, 2023.

Keysight's View of 2023 Threats

We expect that there will be three main target areas in 2023:

- Ransomware
- Internet of Things (IoT)
- Artificial Intelligence (AI)

Ransomware will continue its dirty work

Ransomware attack vectors will continue to be the most impactful security threat of the year for most enterprises. Threat actors have succeeded with successful deployments and monetizing the attacks.

The LockBit 3.0 builder was leaked on Twitter September 21, 2022 (although a copy of the builder was available as early as the beginning of September) for would-be attackers to play with and weaponize. This provided an excellent opportunity for malicious actors to leverage their ransomware easier than ever.

The leak correlates with Keysight's honeypot observation of a ransomware spike in September 2022, as shown in Figure 20 below.

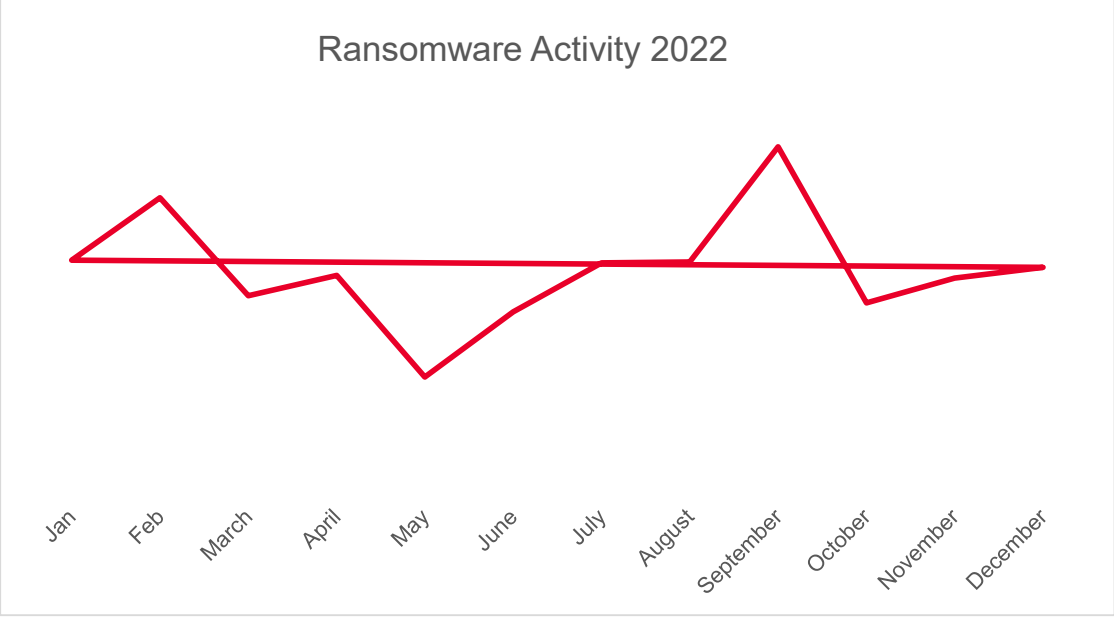

Figure 20. Ransomware activity across 2022

For 2023, we are predicting steady ransomware activity, but not necessarily tied to big groups. However, the leak of multiple ransomware builders and red-teaming tools (such as Brute Ratel and CobaltStrike in the past) will help threat actors to leverage new families of malware and campaigns.[13]

Additionally, we expect to see an increase in ransomware attacks targeting enterprise virtualization servers and data centers.

IoT security continues to be a challenge

IoT security has been a problem for several years. This will intensify over the next couple years as the immature Matter protocol is deployed. Matter is the new standard to interconnect IoT-enabled devices. The rise of this new protocol includes risks and a new opportunity for threats from attackers.

Indeed, based on our 20 years of experience in network protocol and security testing, Keysight predicts that Matter adoption will be an opportunity for new security breaches against common and sensitive assets. Replacing many protocols (Zigbee, Z-wave, etc.) with a unique new and less mature standard implementation will make room for new and unknown-vulnerabilities.

The fundamental areas of attack will be:

- denial of service (performance or vulnerability)
- compromise (vulnerability)
- espionage and data leak

It will take Matter a few, potentially painful, years to harden. During this time expect various threats and check for new CVEs that address the vulnerabilities.

The Dark Knight rises – artificial intelligence bots will increase malicious activity

OpenAI's ChatGPT and other AIs will be a challenge for security operators. At the end of 2022, ChatGPT generated much noise with its capability to write content like a human. Malicious actors already embrace this platform to enhance phishing attacks and multiply their realism through different languages. ChatGPT can even be used by novices, or script kiddies, for malicious purposes.

Since AI/ML is a very active and competitive market, the race is on to demonstrate capabilities. This competition will likely allow attackers to rely on these tools to enhance threat sophistication and evade current security controls. As an example, current phishing mitigation rules should be considered as deprecated, and the rule to check misspellings and lousy sentence structure to identify phishing attempts will be less effective due to tools like ChatGPT.

13 Lawrence Abrams, LockBit ransomware goes 'Green,' uses new Conti-based encryptor, Bleeping Computer, February 1, 2023.

Conclusion

This report concludes with the following key takeaways:

1. Ransomware will be a constant threat that must be addressed ahead of time by IT security departments
2. AI is being weaponized by bad actors to improve their various threat vectors
3. You cannot defend against what you cannot see – you must deploy network visibility and breach and attack simulation technology

Ransomware security attack successes are an indicator of a weakness in most enterprise security architectures — along with the fact that humans (users through email phishing attacks) continue to be a weak link in the security chain. The first key conclusion from this report is that since ransomware will be a constant threat, IT security departments must address the threat ahead of time. This means having a prepared protocol ahead of time that describes how security engineers will need to react to a suspected ransomware threat.

For instance, are data backups being created? If so, how often? In addition, where are backups being stored so that a bad actor can't get to them? When should security engineers restore data to the network from those backups? Should a backup of the network be created of the infected, or suspicious, current network configuration and what are the handling procedures for that specific backup? These data storage concerns need to be documented and addressed long before an attack is recognized.

The general IT security response plan should also be validated and/or updated to specifically address ransomware issues. For instance, how should a potential attack be handled and mitigated? Here are a few example issues to address:

- Should the network be immediately shut down and who is authorized to make this type of decision?
- What isolation techniques can be deployed?
- How should ecommerce transactions and records be handled?
- How often should the network be investigated for a potential ransomware attack, i.e. how often should specific breach and attack (BAS) and threat hunting activities be performed?
- If there is a standby network available (either active load sharing, active / standby, or cold standby), when should this be engaged to isolate the security threat but still preserve business continuity?

A second conclusion is that since artificial intelligence is being weaponized by bad actors to improve their various threat vectors, you need to start preparing for this threat now. AI will probably be used to create autonomous attacks, especially when combined with the compute power of cloud computing networks.

In addition, AI lowers the skill level required for a would-be cybercriminal. Instead of engaging in proof of concepts (POC) to gain knowledge about systems, they can build malware attack scripts much easier using ChatGPT or some other AI system. These attacks will be created that are based on the cyber kill chain model; with each step being automated. Different evasions can also be created by AI solutions to create multiple malware variants with little time or effort required. This will make it much harder to stop an attacker.

In addition, AI will make it easier and faster to run spear phishing campaigns. The AI will be able to gather website and web link information that is tuned to individual people. This allows for better (more personalized) attacks designed to convince people to give up additional personal information and credentials.

At the same time, one benefit from AI is that the security engineer can use the technology as well to automate BAS solutions and (potentially) threat hunting solutions. This empowers the engineer with a force multiplier and enables them to constantly look for signs of lateral movements, C&C, etc.

The third conclusion is that since you cannot defend against what you cannot see, you need to deploy network visibility technology immediately to expose security threats. The first step is to accurately capture and validate potentially suspicious packet data. Flow data and log data can, and should, also be used in threat analysis. However, both of these data sources have challenges. For instance, flow data provides only group and general data observations. While log data has more detail than flow data, specific malware threats can delete or corrupt log data and files — allowing certain threats to slip by unnoticed.

Packet data, however, doesn't lie. It is a consistent source of truth and needs to be utilized as such, even though it requires more work. Taps and packet brokers allow you to collect the packet data across your network, filter it to capture just the data you need, and then pass that data on to one or more security tools for data analysis.

In addition, your network will need continuous breach and attack testing. Annual penetration testing and quarterly cyber range red team/ blue team testing aren't good enough anymore. Not to say those activities should be eliminated, but additional proactive testing with a BAS solution should be included as well.

Good luck with your efforts. If you need help, Keysight Technologies is always available.

About the ATI Research Center

The Keysight ATI Research Center is an elite group of dedicated network security professionals. Its purpose is to stay current with ever-evolving changes that could impact the security of IT networks. The team then distils that knowledge into research which can be incorporated within Keysight solutions to keep up with continually evolving threats.

The ATI team is distributed across the world in locations like Singapore, California, Texas, Massachusetts, France, Romania, and India so that there is always a part of the team that is looking for new threats to analyze.

The ATI team also contributes to the larger security community. It is not just about us. Our team also shares what we learn with vendors that have been hacked, private agencies (e.g. www.mitre.org), government agencies (e.g. NIST and DARPA), and global security conferences like Black Hat and RSA. Keysight also promotes a summer security school in Bucharest, Romania to help train new security engineers.

The key goal for the ATI team is to assess and validate products that are meant to secure the enterprise. We do this by serving as a front line of defense to keep products from other vendors honest. Security alerts and incidents happen all over the globe and the team needs to be up around the clock. Dozens of