SANS Malware & Ransomware Solutions Forum

July 24, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Jake Williams

Sponsored by: Cyberinc, Akamai, VMRAY, Malwarebytes, Cisco Umbrella

AGENDA

10:00 - 10:30am	**Join Slack Workspace (https://join.slack.com/t/sansmalwarera-ecr5129/shared_invite/zt-fymrahd1-ilRMCMgEkx1jWo9sHdUMmA) & Virtual Event (https://www.sans.org/webcasts/112765)**
10:30 - 10:50am	**Welcome & Keynote** As organizations continue to deal with emerging threats in the malware space, its easy for some to take a complacent view and say malware havent we done this already? Weve been dealing with this for decades. And while people who take this view arent wrong we have been dealing with malware for decades the threats are evolving and so must our defenses and strategies. The rise and evolution of ransomware is a great example of just such a progression. In the early days of ransomware, individuals were disproportionately impacted. The vast majority of businesses were well prepared to deal with a single machine (or even a few machines) infected through drive by downloads. Just have good backups and youll be fine. While that might have been true, it is true no more. Ransomware operators have upped their game, adopting APT style tactics and learning evasion techniques from traditional malware authors. The state of play in the malware and ransomware game continues to change at a rapid pace. Those who are still trying to defend against yesterdays threats will find themselves woefully unprepared to deal with the attacks of today. Those same slow movers are likely to be devastated by whatever comes next. Security vendors have helped defenders by innovating with new classes of solutions that didnt exist even a few short years ago. *Jake Williams, @MalwareJake, Forum Chairperson & SANS Instructor*
10:50 - 11:25am	**The Age of Awkward Online Meetings: How Attackers Are Targeting Our Employees Where We Least Expect** What is it about a major global event that makes attackers target victims more successfully? Well for one, all eyes and minds are focused in on that event, whatever it may be. Attackers use that as a relevant way to trick unwitting users into doing bad things. For example, clicking on a link they received through social media that supports or opposes the popular viewpoint, or (as we've seen a lot in the past) around tax season, the amount of IRS and Tax Return related phishing campaigns rise dramatically. In this talk, I'll be looking at some key tactics, techniques and procedures attackers are using as they target victims who are working from home and supporting their companies business operations while trying their best not to put those same business operations at risk. We'll also look into two key concepts: one based around massively distributed attack campaigns and how they work, and two, the concept of Adversarial Resiliency and how "thinking like an attacker" can help your business keep the lights on, even from home.. *Tony Lauro, @TonyLauro, Director of Technology & Security Strategy, Akamai*
11:25am - 12:00pm	**Stopping Ransomware with DNS** The session is focused on the ways DNS can be used to improve protection against ransomware campaigns and speed up investigations of such incidents. We will cover fresh TTP's used by ransomware actors which actively adopt APT style tactics and evasion techniques. Their goal shifted from deploying ransomware on few vulnerable machines to achieving persistence in the network and cause maximum damage to push victims into paying ransom. We will share DNS based classifiers developed by Umbrella team and our approach in building them based on changes in the threats landscape. *Artsiom Holub, @CiscoUmbrella, Senior Security Analyst, Cisco Umbrella*

SANS Malware & Ransomware Solutions Forum

July 24, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Jake Williams

AGENDA

12:00 - 12:35pm	**Defense Against the Dark Arts: Dissecting Sandbox Evasion Techniques** When traditional security products fail in preventing malware from infiltrating an organization, a malware sandbox is often the last hope. For years, malware authors have found ways to stay one step ahead in the arms race with sandbox vendors in this crucial security layer. Building on years of research, the VMRay team tracked and analyzed the sandbox evasion techniques that these malware authors use. Join the VMRay Team, Solutions Engineer Ben Abbott, Senior Threat Analyst Tamas Boczan, and Threat Researcher, Pascal Brackmann, as they take a deeper look at the techniques malware authors use to evade automated dynamic analysis, and what steps can be taken for organizations to restore hope in their defenses. This webcast will explore the following evasion techniques: • Detecting the presence of a sandbox: Once a malicious file detects the presence of a sandbox during execution, it alters its behavior in an effort to avoid being detected. • Exploiting weaknesses in the underlying sandbox technology: This approach typically takes advantage of the fact that most sandboxes use agents, or hooks, to monitor malware activity. • Using contextual triggers: This approach gathers information about the malware's context, such as localization or time, and doesn't execute the malicious behavior unless the malware is running in the right context. *Ben Abbott, @VMRay Solutions Engineer, VMRay* *Tamas Boczan, @tamas_boczan, Senior Threat Analyst, VMRay* *Pascal Brackmann, @VMRay Threat Researcher, VMRay*
12:35 - 12:45pm	**Break & Trivia for $125 Amazon Gift Card**
12:45 - 1:20pm	**Isolation: One Small Step, One Giant Leap** It's almost 50 years since the first dawn of malware in 1971. That it's still a challenge today will come as no surprise to those who live it every day. It's an accepted fact of life. Of course, it's evolved in terms of design, delivery, distribution, and even on-going support. There's been no shortage of silver bullets over the years. As malware has evolved, so have the solutions. So what's new today? The world's a different place today than even 6 months ago. Remote working is an accepted normal (where possible), cloud applications are front-and-center irrespective of the industry, and the browser is the defacto endpoint for many applications and users. It's time to revisit that old foe and see how it's evolving and understand if we can and need to do something different to minimize its impact today. Malicious attacks have cost the US economy anywhere between $57 to $109 billion. The global impact runs in trillions. As we use the Internet every day, we continue to expose our endpoints and our businesses to various types of malware - ransomware, crypto-mining threats, rootkits, and more. Safeguarding against these ever-changing threats requires rethinking our approach to security. In a battle of security vs. productivity, productivity wins more often than we might like. But it needn't always be a battle. Solutions that can open access to the users while safeguarding them can balance security with productivity, and allow our very own end-user (and security practitioner) "superheroes" to each achieve their successes in their battle against the real foe. *Rajiv Raghunarayan, @raraghun, SVP, Products & Marketing, Cyberinc*

SANS Malware & Ransomware Solutions Forum

July 24, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Jake Williams

AGENDA

1:20 - 1:55pm	**Top Three Ransomware Assumptions** Ask most business leaders and they will articulate three ransomware "truths" that guide their priority and preparedness for a ransomware attack. In this session, Malwarebytes will explode these assumptions and provide some best practices for an active defense against ransomware, particularly in today's challenging times. *Michael Williams, @Malwarebytes, Senior Global Product Marketing Manager, Malwarebytes*
1:55 - 2:00pm	**Closing Statement & $125 Gift Card Winner Announced** *Jake Williams, @MalwareJake, Forum Chairperson & SANS Insturctor*