CYBERTHREAT

2019

AGENDA

#CyberThreat19

National Cyber Security Centre

SANS EMEA

25 - 26 NOVEMBER | RIVERBANK PARK PLAZA, LONDON

DAY 1 - MONDAY 25 NOVEMBER

08:00 - 08:45	**Registration and Coffee**
08:45 - 09:00	**Welcome and Introductions** **Carole Theriault - Podcast Host and Producer - Smashing Security and The Cyberwire** **James Lyne - CTO, SANS** **Paul Chichester - Director of Operations, NCSC** **Stephen Jones - Managing Director UK, SANS Institute**
09:00 - 09:40	**Keynote Session** **Scott Helme - Security Researcher**
09:40 - 10:40	**09:40 - 10:40 - CTF & Hackathon** All registered teams to assemble in the designated pods. CTF 101 - A chance for attendees new to Capture The Flag challenges to hear from the technical team that develop our challenges and to learn about the tools and approaches commonly used to solve them. A great preparation for tackling this year's CTF.
	09:50 - 10:10 - Lightning Talk: Mandiant IR: Grab Bag of Attacker Activity We have carefully selected case studies from Incident Response engagements that we have worked on over the last year. You will gain an insight into creative tactics, techniques and procedures (TTPs) seen across the globe, and how we have detected advanced attackers in enterprise environments. Hear about nation state attackers and crime groups such as the newly promoted APT41, publicly known as WINNTI and tracked by Mandiant since 2012, how they have adapted more recently in 2019, as well as other groups we are responding to. **Mitchell Clarke - Incident Response Consultant, UK&I, Mandiant** **Tom Hall - Principle Consultant, Incident Response, Mandiant**
	10:10 - 10:30 - It's Not Just PlayBooks. Enhancing Orchestration with CTI This talk will present different approaches to orchestrating, automating and integrating both the technologies/security infrastructure and people/teams within companies that are too often siloed and disparate. **Chris Jacob, VP Threat Intelligence Engineering, ThreatQuotient**
10:40 - 11:00	**Networking Break** Drinks and snacks will be served

11:00 - 11:30	**Need for PLEAD: BlackTech Pursuit** From abusing valid certificates stolen from prominent organisations, to supply-chain attacks, espionage threat actor BlackTech - tracked by PwC as White Griffin - has upped its sophistication in the past year. Among a wide toolset, BlackTech is known for its unique use of malware family, PLEAD (also known as Bluether and TSCookie). In mid-2019, PwC identified a new campaign using samples of PLEAD. In this talk, we'll conduct a technical comparative analysis of how the PLEAD downloader and backdoor evolved across time and campaigns, providing relevant indicators of compromise and analysing historical samples gleaned from PwC's internal intelligence and open-source reporting. And we'll describe how in investigating this latest campaign, we uncovered links dating back as far as 2014, between White Griffin and another actor that were so far thought to be separate entities. This talk will shine a different light on the threat actor behind the PLEAD toolset and related campaigns, while offering attendees a new direction in which to track this threat actor in the future. It will highlight the nature of attribution as an assessment at a given point in time, and present to attendees for discussion - with reference to our own first-hand experience - the value of applying new knowledge and visibility to older intelligence and intrusion sets, to enrich the picture and validate or reconsider conclusions, in a critical higher-level reflection on the analysis process behind attribution. **Sveva Vittoria Scenarelli - Cyber Threat Intelligence Analyst, PWC UK** **Rachel Mullan - Lead for Strategic Cyber Threat Intelligence, PWC UK**
11:30 - 12:00	**DNS: From Hijacking to Intelligence Apparatus Building** This talk will first take a retrospective look at the techniques, tactics and procedures along with what's, why's and how's of a DNS espionage campaign from 2018 and 2019. This analysis will include a summary the work we did within NCSC to understand the global underpinnings of DNS from registries, registrars, name server operators to anycast providers in order to ascertain its attack surface. We will then then go on to discuss the design, implementation and effectiveness of the framework we built in response to detect indicators of interest from both DNS directly and other sources. The techniques developed can be used to aid in the detection of hijacking, as seen in the DNS espionage campaigns, as well as various other actors and techniques. We will show the data sources, how we ingest, enrich and consume. We will also provide a qualitative analysis of its efficacy. Finally, we'll share a few other analyst techniques we've identified along the way for investigating bad actor use of DNS. **Thomas G - Head of Industry Analysis, NCSC Operations London** **Ollie Whitehouse - Global CTO, NCC Group (and also part of Industry 100 within NCSC Operations London)**
12:00 - 13:00	**Lunch & Vendor Networking** Lunch is served onsite to maximise interaction and networking opportunities among attendees and vendors.

13:00 - 13:45	**MITRE ATT&CK: The Play at Home Edition** You've seen the tactics and techniques. You've read the descriptions. However, something is missing...how do you take the theory of MITRE ATT&CK™ and actually DO something with it? At first glance, it is easy to be overwhelmed by the ATT&CK framework. Where do you start? Who should use it? What can you really do with a framework like ATT&CK? Katie will teach you how to take ATT&CK from a cool-sounding idea to a powerful force for creating a threat-informed defense in your company. She will walk through the story of how ATT&CK helped a fictional organization solve real-world-inspired problems – as well as the struggles they faced along the way and how they overcame them. The presentation will discuss how different teams like threat intelligence analysts, defenders, red teamers, and even executives can use ATT&CK to improve how they track threats and protect against them. Regardless of their role, attendees will learn how they can hit the ground running with ATT&CK on the first day they return home. **Katie Nickels, MITRE ATT&CK Threat Intelligence Lead & SANS Instructor**
13:45 - 14:30	**Using Threat Models for Incidents; Introducing the Possible and Impossible Attack Trees.** In this session we will be talking about why there is a place for threat modelling during incidents, how it's done and how to use it to support your incident detection, investigation and remediation efforts. The session will start with a quick introduction to threat modelling and how it's traditionally used, we'll then move on to how it can be used during an incident. We'll be walking through a couple of different real-world incident scenarios. How threat models and even attack trees can be used to speed up the incident investigation and guide remediation efforts with a focus on sharing how application security and software engineering teams can better support incident leads. Attendees will leave with an understanding of how to use threat modelling within their incident process and with some practical examples of where it works (and where it can still be improved!) **Tash Norris, Lead Security Engineer (Cloud & Appsec) Threat Model-er, Photobox Group**
14:30 - 15:30	**14:30 - 15:30 - CTF & Hackathon** All registered teams to assemble in the designated pods
	14:40 - 15:00 - Lightning Talk: Adventures in Threat Tracking **Jeremy Webb - Threat Intelligence Manager, Royal Bank of Scotland**
	15:00 - 15:30 - Cutting the Phishing Line: Using Certificate Transparency Logs and Open Source Search Tools to Detect Phishing Attempts Against your Organisation In 2019, phishing attacks are still the most popular way to infiltrate an organisation's network. What's worse? The techniques used keep getting more and more sophisticated. Since the launch of "Let's Encrypt", and other certificate authorities providing free TLS certificates, attackers have been using trusted certificates to make phishing landing pages look more genuine. This talk will describe how we can use search tools and publicly available certificate transparency logs to help detect and prevent such attacks. **James Spiteri - Solutions Architect, Cyber Security Specialist Global Solutions Lead, Elastic**

15:30 - 16:00	**Networking Break** Drinks and snacks will be served
16:00 - 16:30	**BRONZE UNION: An Unexpected Journey into the DNA of a Targeted Threat Group** Between 2013 and 2019 we have played a seemingly endless game of cat and mouse with the BRONZE UNION threat group (also known as Emissary Panda). This adversary uses an extensive arsenal of tools and methods to achieve their mission, meaning that the odds can be heavily stacked against front-line network defenders and incident responders. This session will provide a detailed blueprint of the BRONZE UNION threat group developed from nearly three years of continuous visibility of the group's network intrusions and threat campaigns. The session will chart how the group continuously evolves its behaviours to overcome defensive hurdles, and frequently develops its operational approach to remain successful over time. Through dissecting the inner workings of BRONZE UNION's operations we will offer insight into the effective application of threat intelligence, and aim to provide actionable recommendations that all network defenders can use to successfully defend against threats of this calibre. **Matthew Webster - Senior Threat Researcher Counter Threat Unit (CTU), Secureworks** **Mark Osborn - Mark Osborn, Senior Researcher Counter Threat Unit (CTU), Secureworks**
16:30 - 17:00	**How do you do Incident Response for your Azure Active Directory?** Few customers have a rich set of incident response and compromise recovery processes when it comes to their Windows Server Active Directory. Even fewer have matured this process to include Azure Active Directory. This is a big problem, as more and more resources are moving to the cloud. It's not a matter of if a compromise happens, it's a matter of when. In this talk, we will focus on some newly developed guidance from Microsoft on how to do incident response and compromise recovery for Azure Active Directory. This guidance includes attack detection and remediation, recovery steps and recommendations to prevent common attacks from happening in the first place. **Thomas Detzner - Senior Program Manager, Microsoft** **Mark Morowczynski - Principal Program Manager, Microsoft**
17:00 - 17:15	**Closing Remarks** **James Lyne - CTO SANS** **Paul Chichester - Director of Operations, NCSC**
17:45 - 22:00	**Social Activity**

DAY 2 - TUESDAY 26 NOVEMBER

08:00 - 08:45	**Networking and Coffee**
08:45 - 09:00	**Day Two Kick-Off and Coordination Items** **James Lyne - CTO, SANS** **Paul Chichester - Director of Operations, NCSC**
09:00 - 09:40	**Keynote Session** **Deborah Haynes, Foreign Affairs Editor, SKY News**
09:40 - 10:40	**09:40 - 10:40 - CTF & Hackathon** All registered teams to assemble in the designated pods
	09:50 - 10:10 - Lightning Talk: Why Attackers Should Avoid C# **Alex Davies - Senior Security Researcher, F-Secure**
10:40 - 11:00	**Networking Break** Drinks and snacks will be served
11:00 - 11:30	**IR Practitioner's Guide for Setting Organisations up for Success** Dealing with a complex intrusion is hard, both as an incident response provider and as a victim organisation. Stakes are high, victims are under pressure, timelines are short, and it's your job to set up the incident response operation for success. This talk is a practitioner's guide for approaching complex incident response operations where attackers are entrenched, may have had access for years, and maintain the highest level of privilege within victim networks. We'll share our strategies including examples of what has worked and lessons learnt, so that both IR practitioners and victim organisations are better prepared to respond to intrusions. **Mitchell Clarke - Incident Response Consultant, UK&I, Mandiant** **Tom Hall - Principal Consultant, Incident Response, Mandiant**

11:30 - 12:00	**The Case of the Great Firewall** The talk will have a Sherlock Holmes theme. A customer of Cisco had connectivity issues when attempting to use their VPN over the Internet. At first the lack of connectivity appeared to be a misconfigured device, however after troubleshooting, it became apparent that all was not as it had initially appeared. We will guide the audience through the journey we took, using the same techniques we used to determine that the device was not misconfigured, but an on-network device was denying connectivity. We shall - provide an understanding of the VPN protocol (at an RFC level.) When we understand the protocol we can make informed decisions when viewing device debugs we can fully understand protocols flows. When looking at packet captures using Wireshark using these tools we can make an assumption as to what exactly was occurring and how this on-network device functions. Finally we can determine the physical location of the network device performing a man-in-the-middle attack based on network telemetry and the speed of light! The audience should take away the following facts; Debugs, packet captures and decodes are factual. Network analysis requires knowledge of protocol and a fine eye for detail. Once you eliminate the impossible, whatever remains, no matter how improbable, must be the truth. **Gareth Owen - Enterprise Network Security Engineer, Potato Ltd** **Graham Bartlett - Senior Technical Leader, Cisco**
12:00 - 13:00	**Lunch & Vendor Networking** Lunch is served onsite to maximise interaction and networking opportunities among attendees and vendors
13:00 - 13:30	**Scanning for Your Call Records** The Winnti malware family has been deployed in targeted intrusions since 2009 and has been used by a loosely affiliated group of threat actors. The malware has largely been deployed to support wide-scale supply chain compromises, across a wide range of industries and countries. It is used by multiple threat actors whose open source names include Axiom, BARIUM, LEAD, Wicked Panda and GREF. In 2019, game companies again came under attack using Winnti malware. Analysis of these campaigns determined it was likely linked to the 2011 campaign. It has also been in continuous use against other commercial entities. The activities observed in 2019 consist of systematic targeting of telecommunications service providers, government, religious / dissident communities, academia and commercial organisations. Scanning for your call records This presentation will delve into the technical analysis of recent winnti malware and our results scanning for victims. We will also provide analysis of the victimology and possible motives, and our experience with notifying victims of this attack. The key takeaways from this presentation include a brief history of the Winnti Malware, technical analysis of Winnti Malware, Victimology and our experience on notifying victims and lessons learned. **Jason Smart - Lead for Technical Cyber Threat Intelligence, PwC UK** **Kris McConkey - Lead for Cyber Threat Intelligence, Threat Detection & Incident Response, PwC UK**

13:30 - 14:00	**How Actors Respond to Disclosure – Perspectives from Government and Industry** **Recent years have seen an increase in exposures of malicious cyber activity ranging from industry reports, to indictments, attributions, disruptions and sanctions. The UK government has pursued a policy of working alongside allies and partners to do public attributions; cyber criminality is increasingly subject to law enforcement interventions; and teams from both government and industry have worked to shine a light on malicious cyber activity. This presentation will seek to set out some of the ways in which cyber actors respond – both from the perspective of Government and Industry.** **Eleanor Fairford - Deputy Director Cyber Assessment, NCSC** **James Muir - Threat Intelligence Analyst, BAE Systems**
14:00 - 15:00	**14:00 - 15:00 - CTF & Hackathon** All registered teams to assemble in the designated pods
	14:10 - 14:30 - Lightning Talk: Tracking Actors using Banking Malware through their Webinjects **James Wyke - Principal Security Researcher Threat Intelligence, FireEye**
15:00 - 15:30	**Networking Break** Drinks and snacks will be served
15:30 - 16:00	**Tactics, Techniques, and Procedures of the World's Most Dangerous Attackers** In recent years, we have analysed some of the most significant cyberattacks in history. In this presentation we'll go over the most interesting tactics, techniques, and procedures of the adversaries behind them. Specifically, we'll analyse the TTPs of Sednit (a.k.a APT28), the group reportedly responsible for the Democratic National Committee hack that affected the US 2016 elections. The most notable addition to their arsenal is a UEFI rootkit to achieve persistence on victimised systems. Dubbed Lojax, it is the first UEFI rootkit found in the wild. We'll analyse how it works and share the story of its discovery. The second group that we'll focus on is Telebots (a.k.a Sandworm), the group behind the first malware-driven electricity blackouts (BlackEnergy and Industroyer) and the most damaging cyberattack ever (NotPetya). We'll recap these infamous attacks, but also discuss their more recent activities. The discussed TTPs will be mapped to the MITRE ATT&CK taxonomy and we will share some lessons learned from analysing these attacks, useful in strengthening the security posture of your organisation. **Robert Lipovsky - Senior Malware Researcher, ESET**

16:00 - 16:30	**What do you Get when you Add Military Power, with a Sprinkling of Cat Burglar, and a Pinch of Teenage Temper Tantrum?** Over the last several years we've seen North Korean actors grow considerably in both capability, maturity, and targeting scope. Due to the unique position that the North Korean government is in, we're seeing nation-state level tools being leveraged not just for espionage but also for financial theft with incredibly effective outcomes. This talk will focus on not only their ability to infiltrate targets but also the speed in which they can perform actions on their objectives. The presenters will demonstrate that this growth and their expanded targeting makes North Korean computer network exploitation capabilities a global threat to numerous industry verticals. **Josh Burgess - Global Lead Technical Threat Intelligence Adviser, Crowdstrike** **Chris Pike - Lead Cyber Intelligence Adviser for all of Europe, Crowdstrike**
16:30 - 17:00	**Live Demo** **James Lyne - CTO, SANS**
17:00 - 17:30	**Closing Remarks** **James Lyne - CTO, SANS** **Paul Chichester - Director of Operations, NCSC** **Stephen Jones - Managing Director UK, SANS Institute**
17:30 - 19:00	**Social Activity**

We strive to present the most relevant, timely and valuable content. As a result, this Agenda is subject to change. Please check back frequently for changes and updates.