











More talks to be added shortly.

21 October 22 October

<b>JAMES FORSHAW</b> The .NET Inter-Operability Operation	<b>NOUSHIN SHABAB</b> Spring Dragon APT- A Case Study Of Targeted Attacks on APAC Countries	<b>ZDI TEAM</b> Leveraging VMware’s RPC Interface for Fun and Profit
<b>PAUL RASCAGNERES &amp; WARREN MERCER</b> Modern Reconnaissance Phase by APT – Protection Layer	 <b>BALAZS BUCSAY</b> Trick or XFLTReaT a.k.a. Tunnel All the Things	<b>YANG JUNFENG (@BLUERUST)</b> How I Generically Bypassed CFG
 <b>VITALY KAMLUK</b> Chasing Ghosts In The Wires	 <b>YU HONG (REDRAIN) &amp; MIN (SPARK) ZHENG</b> A Ghost from Postscript	<b>SEAN PARK (SPARKY)</b> Neural Blacklist: Fighting Mutating Polymorphic URLs
<b>HSIEN-DE HUANG &amp; CHIA-MU YU</b> Look! Ransomware Is There: Large Scale Ransomware Detection with Naked Eye	<b>JOHN BIRD</b> In Soviet Russia, Radare2 Debugs You!	 <b>ZINUO HAN</b> A Whole New Efficient Fuzzing Strategy for Stagefright: Porting and Optimizations
<b>AARON FENWICK (MULTIPLEX3R)</b> Hacking SkyNet – Anatomy of an intelligent Industrial Control System	<b>RYAN HOLEMAN &amp; ALEK AMRANI</b> HODOR: Holding Open Doors and Often Reconnecting	<b>TY MILLER &amp; PAUL KALININ</b> The Active Directory Botnet
 <b>TIM KORNAU</b> The many Dimensions of Relationships	<b>BYRNE GHAVALAS &amp; BARTOSZ INGLOT</b> Attacker Antics: Illustrations of Ingenuity	<b>WAYNE RONALDSON</b> Executives In The Red
 <b>FERNANDO ARNABOLDI</b> Embedding Defense in Server-Side Applications	 <b>JOHN DUNLAP</b> Comparison and Improvements for Existing Jump Oriented Programming Tools	<b>PAUL THERIAULT</b> Improving Privacy on the Web
<b>BRANDON DIXON</b> One-click Browser Defense	<b>FRASER TWEEDALE</b> User Session Recording – An Open Source Solution	<b>STEVE GINTY</b> The Mechanized Analyst
<b>DR VANESSA TEAGUE &amp; CHRIS CULNAME</b> Privacy and Big Data	 <b>MINRUI YAN &amp; MINGGE CAO</b> Some Attack Surfaces For Telematics Hardware	

## JAMES FORSHAW

### THE .NET INTER-OPERABILITY OPERATION

One of the best features of the .NET runtime is its in-built ability to call native code, whether that’s APIs exposed from dynamic libraries or remote COM objects. Adding this in-built functionality to a “type-safe” runtime has its drawbacks, not the least the introduction of security issues due to misuse. This presentation will go into depth on how

the .NET runtime implements its various interop features, where the bodies are buried and how to use that to find issues ranging from novel code execution mechanisms, elevation of privilege up to remote code execution. The presentation will assume the attendee has some familiarity with .NET and how the runtime executes code.

## JAMES FORSHAW BIO

James is a security researcher in Google's Project Zero. He has been involved with computer hardware and software security for over 10 years looking at a range of different platforms and applications. With a great interest in logical vulnerabilities he's been listed as the #1 researcher for MSRC, as well as being a Pwn2Own and Microsoft Mitigation Bypass bounty winner. He has spoken at a number of security conferences including Black Hat USA, CanSecWest, Bluehat, HITB, and Infiltrate.

---

## NOUSHIN SHABAB

### SPRING DRAGON APT- A CASE STUDY OF TARGETED ATTACKS ON APAC COUNTRIES

n the beginning of 2017, Kaspersky Lab became aware of new activities by an APT actor we have been tracking for several years called Spring Dragon (also known as LotusBlossom).

Spring Dragon is a long running APT actor that operates on a massive scale. The group has been running campaigns, mostly in countries and territories around the South China Sea, since as early as 2012. The main targets of Spring Dragon attacks are high profile governmental organisations and political parties, education institutions such as universities, as well as companies from the telecommunications sector.

Spring Dragon is known for spear phishing and watering hole techniques. We collected a large set (600+) of malware samples used in different attacks, with customised C2 addresses and campaign codes hardcoded in the malware samples.

This presentation will focus on the evolution of Spring Dragon tools and dive into their TTPs (Techniques, Tactics and Procedures) to reveal the capabilities of this APT actor.

## NOUSHIN SHABAB BIO

Noushin Shabab is a cyber security researcher based in Australia specialising in malware reverse engineering and targeted attack investigations. She joined Kaspersky Lab in 2016 as a Senior Security Researcher in Global Research & Analysis Team (GReAT). Her research focuses on the investigations of advanced cyber criminal activities and targeted attacks with primary focus on local threats in APAC region. Prior to joining Kaspersky Lab, Noushin also delved in malware analysis, security research and software development for a security software company overseas. She has first-hand knowledge of rootkit analysis and detection techniques as well as APT malware analysis.

---

## ZDI TEAM



### LEVERAGING VMWARE'S RPC INTERFACE FOR FUN AND PROFIT

Virtual machines play a crucial role in modern computing. They often are used to isolate multiple customers with instances on the same physical server. Virtual machines are also used by researchers and security practitioners to isolate potentially harmful code for analysis and review. The assumption being made is that by running in a virtual machine, the potentially harmful code cannot execute anywhere else. However, this is not foolproof, as a vulnerability in the virtual machine hypervisor can give access to the entire system. While this was once thought of as just hypothetical, two separate demonstrations at Pwn2Own 2017 proved this exact scenario.

This talk details the host-to-guest communications within VMware. Additionally, the presentation covers the functionalities of the RPC interface. In this section of the presentation, we discuss the techniques that can be used to record or sniff the RPC requests sent from the Guest OS to the Host OS automatically. We also demonstrate how to write tools to query the RPC Interface in C++ and Python for fuzzing purposes.

Finally, we demonstrate how to exploit Use-After-Free vulnerabilities in VMware by walking through a patched vulnerability.

## ZDI TEAM BIO

**Brian Gorenc** is the directory of Vulnerability Research with Trend Micro. In this role, Gorenc leads the Zero Day Initiative (ZDI) program, which represents the world's largest vendor-agnostic bug bounty program. His focus includes analyzing and performing root-cause analysis on hundreds of zero-day vulnerabilities submitted by ZDI researchers from around the world.

The ZDI works to expose and remediate weaknesses in the world's most popular software. Brian is also responsible for organizing the ever-popular Pwn2Own hacking competitions.

**Jasiel Spelman** is a vulnerability analyst and exploit developer for the Zero Day Initiative (ZDI) program. His primary role involves performing root cause analysis on ZDI submissions to determine exploitability, followed by developing exploits for accepted cases. Prior to being part of ZDI, Jasiel was a member of the Digital Vaccine team where he wrote exploits for ZDI submissions, and helped develop the ReputationDV service from TippingPoint. Jasiel's focus started off in the networking world but then shifted to development until transitioning to security. He has a BA in Computer Science from the University of Texas at Austin. Twitter: @WanderingGlitch

**Abdul-Aziz Hariri** is a security researcher with the Zero Day Initiative program. In this role, Hariri analyzes and performs root-cause analysis on hundreds of vulnerabilities submitted to the Zero Day Initiative (ZDI) program, which is the world's largest vendor-agnostic bug bounty program. His focus includes performing root-cause analysis, fuzzing and exploit development. Prior to joining ZDI, Hariri worked as an independent security researcher and threat analyst for Morgan Stanley emergency response team.

During his time as an independent researcher, he was profiled by Wired magazine in their 2012 article, Portrait of a Full-Time Bug Hunter. In 2015, Abdul was part of the research team that submitted "Breaking Silent Mitigations – Gaining code execution on Isolated Heap and MemoryProtection hardened Internet Explorer" to the Microsoft bounty program. Their submission netted the highest payout to date from the Microsoft bounty program where the proceeds went to many STEM organizations.

---

## PAUL RASCAGNERES & WARREN MERCER

### MODERN RECONNAISSANCE PHASE BY APT – PROTECTION LAYER

The Talos researchers are no stranger to APT attacks. During recent research, we observed how APT actors are evolving and how the reconnaissance phase is changing to protect their valuable 0-day exploit or malware frameworks. During the presentation, we will not speak about a specific malware actor but we will use various different cases to illustrate how the reconnaissance phase is becoming more important and more complex.

This talk will mainly focus on the usage of malicious documents (Microsoft Office and Hangul Word Processor) and watering hole attacks designed to establish if the target is the intended one. We will mention campaigns against political or military organizations targeting USA, Europa and Asia.

The techniques and the obfuscation put in place by these actors will be described in detail. We will explain how the Macros are used and how to desobfuscated them; how the JavaScript and the PowerShell are becoming unmissable languages and how to analyse these languages with standard debugger such as WinDBG; how APT actors includes Flash objects in document to bypass protection and perform reconnaissance on the target; finally, we will see how Python language is used by malware to execute code on MacOS. In some cases, the reconnaissance is performed directly by a first stage malware (PE32) and not directly by the infection vector, we will see an example of the approach that targeted South Korea public sectors at the end of December.

At the end of the presentation, we will show different mitigations in applications (for example in Microsoft Office and Hangul Word Processor) and in the Microsoft Windows Operating System to help attendees protect their constituents against the treats described during the talk.

### PAUL RASCAGNERES & WARREN MERCER BIO

Paul is a security researcher within Talos, Cisco's threat intelligence and research organization. As a researcher, he performs investigations to identify new threats and presents his findings as publications and at international security conferences throughout the world. He has been involved in security research for 7 years, mainly focusing on malware analysis, malware hunting and more specially on Advanced Persistence Threat campaigns and rootkit capabilities. He previously worked for several incident response team within the private and public sectors.

Warren Mercer joined Talos coming from a network security background, having previously worked for other vendors and the financial sector. Focusing on security research and threat intelligence, Warren finds himself in the deep, dark and dirty areas of the Internet and enjoys the thrill of the chase when it comes to tracking down new malware and the bad guys! Warren has spent time in various roles throughout his career, ranging from NOC engineer to leading teams of other passionate security engineers. Warren enjoys keeping up to speed with all the latest security trends, gadgets and gizmos; anything that makes his life easier in work helps!

---

## BALAZS BUCSAY

### TRICK OR XFLTREAT A.K.A. TUNNEL ALL THE THINGS

This presentation will sum up how to do tunnelling with different protocols and will have different perspectives detailed. For example, companies are fighting hard to block exfiltration from their network: they use http(s) proxies, DLP, IPS technologies to protect their data, but are they protected against tunnelling? There are so many interesting questions to answer for users, abusers, companies and malware



researchers. Mitigation and bypass techniques will be shown you during this presentation, which can be used to filter any tunnelling on your network or to bypass misconfigured filters.

Our new tool XFLTRaT is an open-source tunnelling framework that handles all the boring stuff and gives users the capability to take care of only the things that matter. It provides significant improvements over existing tools. From now on there is no need to write a new tunnel for each and every protocol or to deal with interfaces and routing. Any protocol can be converted to a module, which works in a plug-and-play fashion; authentication and encryption can be configured and customised on all traffic and it is also worth mentioning that the framework was designed to be easy to configure, use and develop. In case there is a need to send packets over ICMP type 0 or HTTPS TLS v1.2 with a special header, then this can be done in a matter of minutes, instead of developing a new tool from scratch. The potential use (or abuse) cases are plentiful, such as bypassing network restrictions of an ISP, the proxy of a workplace or obtaining Internet connectivity through bypassing captive portals in the middle of the Atlantic Ocean or at an altitude of 33000ft on an airplane.

This framework is not just a tool; it unites different technologies in the field of tunnelling. While we needed to use different tunnels and VPNs for different protocols in the past like OpenVPN for TCP and UDP, ptunnel for ICMP or iodined for DNS tunnelling, it changes now. After taking a look at these tools it was easy to see some commonality, all of them are doing the same things only the means of communication are different. We simplified the whole process and created a framework that is responsible for everything but the communication itself, we rethought the old way of tunnelling and tried to give something new to the community. After the initial setup the framework takes care of everything. With the check functionality we can even find out, which module can be used on the network, there is no need for any low-level packet fu and hassle. I guarantee that you won't be disappointed with the tool and the talk, actually you will be richer with an open-source tool.

## BALAZS BUCSAY BIO

Balazs Bucsay (@xoreipeip) is a Senior Security Consultant at NCC Group in the United Kingdom who does research and penetration testing for various companies. He has presented at many conferences around the world including Honolulu, Atlanta, London, Oslo, Moscow, and Vienna on multiple advanced topics relating to the Linux kernel, NFC and Windows security. Moreover he has multiple certifications (OSCE, OSCP, OSWP, GIAC GPEN) related to penetration testing, exploit writing and other low-level topics; and has degrees in Mathematics and Computer Science. Balazs thinks that sharing knowledge is one of the most important things in life, so he always shares his experience and knowledge with his colleagues and friends. Because of his passion of technology, he starts his second shift in the evenings, right after work to do further research.

## YANG JUNFENG (@BLUERUST)

### HOW I GENERICALLY BYPASSED CFG

Over the years, Microsoft has introduced many forms of exploit mitigation in an effort to drive up the costs of exploitation. In Windows 10, Microsoft introduced the control flow guard (CFG) mitigation, further increasing the difficulty of exploitation on the Windows platform. However, as history has shown, nothing is perfect. Even though CFG has already been around for some time and many researchers have contributed to improving CFG, subtle flaws still exist.

In this talk, I will present several amazing exploitation techniques which bypass CFG easily and generically, given a read/write primitive – something not uncommon in modern exploits. These techniques I will share can be applied to exploit various software such as Edge, IE, Adobe Reader, Flash and Microsoft Office. I will also share some exploitation tricks I have developed, some of which are novel enough to earn bounties with Microsoft's Mitigation Bypass programme.

## YANG JUNFENG (@BLUERUST) BIO

Yang Junfeng is currently a staff researcher at DiDi Research America. He previously worked at NSFOCUS and FireEye as a vulnerability researcher. Junfeng has a keen interest in anything security and especially exploitation. He received a bounty from the Microsoft Mitigation Bypass programme for his contributions. ( Bounty Hunters: The Honour Roll <https://technet.microsoft.com/en-us/security/dn469163.aspx> )

## VITALY KAMLUK

### CHASING GHOSTS IN THE WIRES

Kaspersky Lab research team has spent almost a year tracking an elusive threat actor that was responsible for one of the biggest cyber heists in history: Bangladesh Central Bank attack, which resulted in \$81 mln USD theft with initial target over \$951 mln USD. Some time after Bangladesh incident, we discovered the attackers in few other unusual places around the world and interrupted their attempts to steal large amounts of money.

This talk will focus on advanced custom tools and smart techniques used during the attacks. Many of those tools and techniques rendered





traditional incident response and forensic analysis useless. The presentation will contain answers of how such problems should be addressed in a better way. Considering that the attackers are still out there “in the wires”, the presentation will conclude with our top recommendations to all potential targets.

While the presentation will be based on specific investigation, it contains valuable general insights into what a modern top-notch cyberattacks look like.

### VITALY KAMLUK BIO

Vitaly has been involved in malware research at Kaspersky Lab since 2005. In 2008, he was appointed Senior Antivirus Expert, before going on to become Director of the EEMEA Research Center in 2009. He spent a year in Japan focusing on major local threats affecting the region. In 2014 he was seconded to the INTERPOL Global Complex for Innovation in Singapore, where he worked in the INTERPOL Digital Crime Center specialising in malware reverse engineering, digital forensics and cybercrime investigation.

Prior to joining Kaspersky Lab, Vitaly worked as a software developer and system administrator. He is a graduate of the Faculty of Applied Math and Computer Science at the Belarussian State University

Vitaly has presented at many public international security conferences including Blackhat USA, Blackhat Asia, Defcon, Hitcon, BSides Las Vegas, PHDays, ZeroNights, FIRST, Source Boston as well as multiple closed door invite-only security industry events such as Underground Economy, DCC, InBot and more.



## YU HONG (REDRAIN) & MIN (SPARK) ZHENG

### A GHOST FROM POSTSCRIPT

PostScript is a programming language introduced by Adobe for image and text printing. Although this language is not well known, it is indispensable for printing. We have studied PostScript and GhostScript (an engine of PostScript) since last year. And we found several interesting security vulnerabilities in them.

In this talk, we first introduce the grammar specification of PostScript and discuss the security weaknesses of this language. After that, we show several vulnerabilities of GhostScript that can cause arbitrary file read, arbitrary code execution and sandbox escape. In addition, we extend our PostScript security study to other well-known image processing software (e.g., ImageMagick, Evince) used GhostScript engine. The result shows that even the latest version of these software still have 0-day vulnerabilities for PostScript language processing.

### YU HONG (REDRAIN) & MIN (SPARK) ZHENG BIO

Yu Hong (redrain) is a Senior Security Researcher at from 360CERT of Qihoo 360. With more than 7 years of experience in security research and web application penetration testing, he has discovered and reported several vulnerabilities and received acknowledgement for his contributions from various companies including Apple, Baidu, Tencent, Alibaba and more. Yu has gave presentations on HITB, hitcon

Min (Spark) Zheng is a security expert @Alibaba mobile security. He received his Ph.D. degree in the CSE department of the Chinese University of Hong Kong. His research focuses on malware analysis, smartphone (Android & iOS) security, system design and implementation. Before receiving Alibaba A-Star offer award in 2015, he worked in FireEye, Baidu and Tencent. He was the champion of GeekPwn 2014 and AliCTF 2015. And his won the “best security researcher” award in FIT 2016, China for detecting the XcodeGhost virus and WormHole vulnerability. His personal interests include films, computer games and CTF (capture the flag).

## SEAN PARK (SPARKY)

### NEURAL BLACKLIST: FIGHTING MUTATING POLYMORPHIC URLS

Latest malware attacks use more and more polymorphic URLs to reduce the chance of being caught on their initial infection sites, malware drop sites and landing pages. For instance, Cryptolocker (a.k.a. Torrentlocker), being one of the most notorious ransomware families, takes random folder and file name as part of the initial infection URL structure. Various Domain Generation algorithms (DGAs) have patterns that human beings easily recognize but the automation finds it hard to detect. RIG-EK, the most popular exploit kit this year, also uses special random patterns in the drop sites. To make matters worse, these polymorphic URL patterns mutate over time, which makes the detection job extremely challenging. From the defender’s perspective, it is crucial to stop users from accessing these malicious URLs in order to break the chain of infection. Traditionally this URL pattern matching has been dealt with by regular expressions and handcrafted algorithms. However, URL polymorphism and constant mutation renders these traditional approaches very costly and unsatisfactory at its best.

Recently deep learning has proven to perform really well especially in recognizing non-linear patterns, which human brain’s neural network is good at. With not much of a surprise, my research shows it also works great at solving highly engineered malicious URLs. In this talk, I will demonstrate how to leverage the state of the art Attention Long Short Term Memory (LSTM) to detect variable length malicious URL patterns. I will also visualize how and why this neural network separates different classes of URLs in such a high accuracy. This work has been evaluated against a large corpus of Akamai logs and the latest malicious URL dataset, and recorded a nearly perfect precision and recall rate. Along with a very short training time, this model also allows us to integrate it into production systems with minimal deployment overhead and maintenance cost.

## SEAN PARK (SPARKY) BIO

Sparky is a senior malware scientist at Trend Micro trying to solve highly difficult problems using deep learning. His main focus is deep learning based threat detection including unsupervised malware clustering using convolutional autoencoder, malware metamorphism detection using Semantic Hashing with Fourier transform, Cryptolocker URL detection using multi-layer gated recurrent unit with attention mechanism, OSX Malware detection using convolutional autoencoder, exploit detection using hierarchical LSTM, real time unsupervised malware email campaign clustering using DBSCAN, and machine learning model benchmarking platform for online In-the-wild samples.

He previously worked for Kaspersky, FireEye, Symantec, and Sophos. He also created a critical security system for banking malware at a top Australian bank.

---

## HSIEN-DE HUANG & CHIA-MU YU



### LOOK! RANSOMWARE IS THERE: LARGE SCALE RANSOMWARE DETECTION WITH NAKED EYE

Ransomware such as WannaCrypt and Petya have caused significant financial loss and even have endangered human life (e.g., ransomware attack on UK hospitals). Ransomware on desktop has gained much attention from academic and industry. However, we see that the number of ransomware on Android phones remains steady increasing, but gains much less attention. As Android has been the most popular smartphone OS and a substantial number of credentials are kept only in smartphones, the data loss incurs serious inconvenience and loss. Here, we present our deep learning-based ransomware detection system, coloR-inspired convolutional neuRal network-based android ransomware Detection (R2D2). R2D2 was originally developed to sweep the malware, but we found it particularly useful in detecting ransomware. A unique feature is its end-to-end training, without human intervention. Such an end-to-end training points out a direction that we no longer need tedious search for roust ransomware features for detection. Most importantly, based on R2D2, we develop techniques to encode ransomware as so-called ransomware image, such that the ransomware from the same family exhibit the same pattern and even non-experts can detect and even determine the ransomware family with their the naked eye.

## HSIEN-DE HUANG & CHIA-MU YU BIO

**Hsien-De Huang** (a.k.a. TonTon) is working for Leopard Mobile (Cheetah Mobile Taiwan Agency). His current major research interests include Deep Learning, Malware Analysis, Android Reverse Engineering, Type-2 Fuzzy Logic, and Ontology Applications. He also is a Ph. D. candidate (IKM Lab.) in the Dept. Computer Science and Information Engineering at National Cheng Kung University, Taiwan. He also was a visiting Ph. D student in the UK for research project “2010 Initiative Research Cooperation among Top Universities between UK and Taiwan” at University of Essex, UK and in the research project “2012 NSC-INRIA International Program – Associate Team (II)” at INRIA Saclay, France. In the past few years, he was a Software Developer at Verint Systems (Taiwan), Senior Security Engineer at Acer e-Enabling Data Center(Acer eDC) and Project Assistant Researcher at the National Center for High-Performance Computing (NCHC). <http://TWMAN.ORG> is his personal website.

**Chia-Mu Yu** received his Ph.D degree from National Taiwan University in 2012. He is currently an assistant professor at National Chung Hsing University, Taiwan. He was a research assistant in the Institute of Information Science, Academia Sinica. He was a visiting scholar at Harvard University, Imperial College London, Waseda University, and University of Padova. He was a postdoc researcher at IBM Thomas J. Watson Research Center. He serves as an associate editor of IEEE Access and Security and Communication Networks. His research interests include cloud storage security, IoT security, and differential privacy.

**Hung-Yu Kao** received the B.S. and M.S. degree in Computer Science from National Tsing Hua University in 1994 and 1996 respectively. In July 2003, he received the PhD degree from the Electrical Engineering Department, National Taiwan University. He is currently the Director of Institute of Medical Informatics and a professor of Department of Computer Science and Information Engineering of National Cheng Kung University. He was a post-doctoral fellow of Institute of Information Science (IIS), Academia Sinica from 2003 to 2004. His research interests include Web information retrieval / extraction, search engine, knowledge management, data mining, social network analysis and bioinformatics.

---

## JOHN BIRD

### IN SOVIET RUSSIA, RADARE2 DEBUGS YOU!

This talk will be all about Radare2 – one of the new reversing/debugging/code analysis offerings on the market. It's fast, capable, opensource, free and its user base is growing quickly.

By the end of this you will (hopefully) be able to navigate some of its core functionality as well as get an overview of its other components (like rabin2, rafind2, ragg2, rasm2 etc).

You will also get to see some CTF challenges being solved <blink>live on stage</blink>. Nah, just kidding – solved them a long time ago...just wanted to see if that blink tag bit would make it into the speakers page. If so there might be a lame XSS vuln. Hmm, lets try this <script>alert('xss')</script>. Yeah, I'll just leave that bit there.

## JOHN BIRD BIO

John is just some /dev/urandom guy. Really – nothing to see here....so move on. He did present in 2013 on GPU cracking password stuff and that went ok... so feel free to rock up.



## ZINUO HAN

### A WHOLE NEW EFFICIENT FUZZING STRATEGY FOR STAGEFRIGHT: PORTING AND OPTIMIZATIONS

In this presentation, I will present how I found several critical vulnerabilities in Stagefright media framework. First of all, I start with a brief overview on the Stagefright security status. Next, I review the previous fuzz strategies and point out their disadvantages. Then, a new efficient fuzz strategy will be presented. The features of the proposed fuzz strategy include: the new attack surface, the porting of multiple core components, as well as a set of special tricks for improving fuzz efficiency. Finally, a dozen of CVEs found by the above method will be shown to you.

From this presentation, you can learn how to reproduce the known vulnerabilities and discover new vulnerabilities in Stagefright more effectively. In addition, these experiences can also be applied to other Android native programs written by C/C++.

## ZINUO HAN BIO

Zinuo Han(ele7enxxh) is a security researcher at Chengdu Security Response Center, Qihoo 360, mainly focus on vulnerability discovery and vulnerability analysis on Android last year. He has rich experiences in File format fuzzing and discovered quite a few vulnerabilities this year.

## AARON FENWICK (MULTIPLEX3R)

### HACKING SKYNET – ANATOMY OF AN INTELLIGENT INDUSTRIAL CONTROL SYSTEM

## AARON FENWICK (MULTIPLEX3R) BIO

Father, Husband, Hacker, Electronics enthusiast and Penetration Tester @ PwC specialising in Operational Technology – I spend my work time travelling around the world to some pretty inhospitable places hacking into Industrial Control Systems for various clients and giving advice to help secure these systems from a practical perspective. I 😞am a Crest CRT, OSCP and OSCE – That being said, I have electrocuted myself more than once

## RYAN HOLEMAN & ALEK AMRANI



### HODOR: HOLDING OPEN DOORS AND OFTEN RECONNECTING

Finding or obtaining user credentials is a fairly simple task and can be done in numerous ways. From writing a 5 line python script that validates credential dumps to using fake login portals to mine credentials. Unfortunately, pesky security teams and automated alerts are becoming more robust and can quickly detect and remediate credential compromise. This remediation can put a damper on using all your shiny new validated credentials.

What if you could use your valid credentials even after a user account reset? This is where Hodor come in. Hodor is a reusable, easy to use framework to assist in holding credential sessions open after a compromise. Built to be generic and reusable, Hodor abuses the fact that credential resets typically don't reset all authentication mechanisms (sessions, temporary credentials, api tokens, etc). On your next harvest, let Hodor help you to overcome your security roadblocks and preserve your hard earned access.

## RYAN HOLEMAN & ALEK AMRANI BIO



**Ryan Holeman** resides in Austin Texas where he runs Atlassian’s Security Intelligence team. He is also an advisor for the endpoint security software company Ziften Technologies. He received a Masters of Science in Software Engineering from Kent State University. His graduate research and masters thesis focused on C++ template metaprograming. He has spoken at many respected venues such as Black Hat, DEF CON, ShmooCon, Lockdown, BSides and Notacon and has published papers though venues such as ICSM and ICPC . You can keep up with his current activity, open source contributions and general news on his blog. His spare time is mostly spent digging into various network protocols, random hacking, creating art, and shredding local skateparks.

**Alek** is part of the Atlassian security engineering team. Self proclaimed AHA! heckler, idiot triathlete, obsessed travel hacker, and CTF connisoeur.

“Doer of things, duder of peoples.” — WanderingGlitch

“Wrecks \$hit, trolling, and heckling. Also runs too much.” — hackgnar

“Some professional words that sound good.” — zxcvbnm

“Actually runs long distances for fun.” — unicornfurnace

---

## TY MILLER & PAUL KALININ

### THE ACTIVE DIRECTORY BOTNET

Botnets and C&C servers are taking over the internet and are a major threat to all of us ... but what happens when these botnets and C&C servers start existing and operating inside the walls of our organisations? What if these botnets and C&C servers could bypass all of our network controls? What if these botnets and C&C servers could communicate internally across our security zones and organisations? What if micro-segmentation suddenly became useless?

This brand new attack technique makes this nightmare a reality by turning your Active Directory Domain Controllers into C&C servers that can command a powerful internal botnet. This attack technique is a fundamental flaw within the way that nearly every organisation implements their Active Directory solution, which leaves a gaping hole within their security and their ability to contain security breaches.

This is achieved by leveraging standard Active Directory attributes and features to force your Domain Controllers to act as a central communication point for all internally compromised systems.

Due to the architecture of nearly every Active Directory implementation on the planet, almost all servers, workstations, laptops, mobile devices, and wireless devices throughout our organisations can connect to a Domain Controller for authentication purposes.

This provides the ability for The Active Directory Botnet to communicate through a network of strategically placed Active Directory C&C servers. This enables all of your firewalls and network access controls to be bypassed through this central authentication mechanism that automatically synchronises our botnet traffic across all of your Domain Controllers throughout your organisation.

This means that our Active Directory Botnet can not only communicate across WAN sites globally, but if your Active Directory is configured to sync to the cloud, then this introduces a whole other level.

So how does the Active Directory Botnet work? Standard Active Directory accounts support over 50 user attributes that can be combined to create a communication channel between any compromised domain machine located throughout your organisation.

The Active Directory Botnet Client injects unique data entries into their corresponding AD account attributes within the target Domain Controller, and begins polling to identify other compromised systems within the domain. At this point, any Active Directory Botnet Client within the domain can identify compromised machines and begin issuing commands to be executed on either individual systems or across all infected endpoints.

The Active Directory Botnet Clients then execute the commands and begin tunnelling the command output back through their corresponding Active Directory account attribute fields, which are then collected by the Active Directory Botnet Client that issued the original command.

Not only does the Active Directory Botnet enable remote command execution for any domain system, it also has the capability to provide a transparent TCP data channel that ultimately turns your entire security architecture into a flat network.

A series of live demonstrations of this attack will be performed during the presentation to show the attack in action, including remote command execution, backdoor uploads, and multiple transparent data transfer techniques.

The primary way of preventing this attack is to lock down access to change standard user attributes in AD, monitor regular changes to Active Directory standard user attributes that are not typically changed on a regular basis, and by rearchitcting security zones to use different Active Directory Forests. This attack is a clear violation of the way that Active Directory is typically used; however, due to the overwhelming insecure architecture implementations of Active Directory, and the difficulty of changing Active Directory architectures, this new attack technique will be effective for many years to come.



## TY MILLER & PAUL KALININ BIO

**Ty Miller** is the Managing Director of Threat Intelligence Pty Ltd ([www.threatintelligence.com](http://www.threatintelligence.com)) who is a Specialist Security Company based in Australia. Ty holds a position on the Black Hat Asia Review Board, the CREST ANZ Board of Directors and leads the CREST Technical Team.

He is a long term trainer for Black Hat running “The Shellcode Lab” and “Practical Threat Intelligence”, and is a presenter at security conferences including Ruxcon, Black Hat USA, Black Hat DC, and Hack In The Box, amongst many others. This includes presenting on “Reverse DNS Tunneling Shellcode” at Black Hat USA, “BeEF Bind Shellcode” at Ruxcon, and others including “Machine Learning and Modern Malware Mitigations”, “Securing Your Startup to Secure Big Brands”, “Modern Threat Detection and Prevention” and “Can your application be breached?”.

Ty has developed attack techniques for global security firms including the “DNS Channel Payload” for Core Impact and is a co-author of “Hacking Exposed Linux 3rd Edition”.

**Paul Kalinin** is a Senior Security Consultant at Threat Intelligence Pty Ltd. Paul has presented his security research at Black Hat and ran the Practical Threat Intelligence training at Black Hat USA.

Paul has been working in the IT industry for 20 years with the last 8 years being dedicated as a security specialist focusing on penetration testing. Paul has achieved a range of industry certifications such as CISSP, PCI QSA, CEH and CREST.

Paul’s areas of expertise include web and mobile application penetration testing, internal and external infrastructure penetration testing, wireless infrastructure penetration testing, red teaming and open source intelligence specialist.

Paul has been a key player in the development of penetration testing tools, exploits, methodologies and cyber threat intelligence gathering within the Threat Intelligence team.



## TIM KORNAU

### THE MANY DIMENSIONS OF RELATIONSHIPS

A presentation about how to use fuzzy executable and function similarity at scale. We will go over past approaches and why they failed. We will describe the general idea of fuzzy executable and function similarity and introduce the basic math concepts behind our approach. We will introduce concepts used for detection on executable and function level. We will show how “close relative” relationships between executables can aid analysts workflows. We will show how “distant relative” relationships can be identified via our approach and how they can be used. We will show how prevalence can be used to further strengthen the approach.

## TIM KORNAU BIO

Tim Kornau is a software engineer at Google Threat Analysis Group. He has previously worked as software engineer at zynamics. Tim holds a Masters from Ruhr University Bochum in IT-Security.

## BYRNE GHAVALAS & BARTOSZ INGLOT

### ATTACKER ANTICS: ILLUSTRATIONS OF INGENUITY

The arms race between the vendors creating security defences and the hackers trying to defeat them continues. While responding to security breaches around the world, we have uncovered some creative and ingenious tactics, techniques and procedures (TTPs). We carefully selected several of the more recent and fascinating attacker TTPs and we are excited to share them with you. Come to the talk to hear about attackers breaching air-gapped networks, abusing an anti-virus server, hijacking victim’s emails, camouflaging malware and preventing it from sandbox execution, and using obscure persistence mechanisms, to name a few.

## BYRNE GHAVALAS & BARTOSZ INGLOT BIO

**Byrne** is a principal consultant at Mandiant. He started out in South Africa, spent 16 years in the UK and now is based in Sydney, Australia. As part of the incident response team, Byrne leads IR investigations of targeted attacks. Byrne is an information security specialist with over 17 years’ experience in the industry, working with federal government, law enforcement, defence industry and Fortune 500 companies across multiple industries. He has extensive experience in incident response, forensic investigations and cyber operations. He is a security geek, climber, sailor, and is partial to good coffee and good wine.

**Bart** is an incident response and forensics specialist in Mandiant's Security Consulting Services team helping clients restore confidence in an event of a breach. He holds a degree in Computer Forensics, is a keen developer, enjoys inspecting network traffic and specialises in Windows forensics with fascination in volatile memory. Having worked on incident response engagements around the world, Bart routinely develops new tools and ideas to solve on-the-job problems and to ensure Mandiant remains an industry leader. Some of these developments led to Bart's contributions to the Volatility project. After spending 8 years in England, Bart recently relocated to South-East Asia as he believes it's still the most fascinating, culturally diverse, and opportunistic region in the world. The relative immaturity in Cyber Security in most countries, but also the "hunger to learn" that most businesses and government organizations display, offer a significant growth opportunity.

---

## WAYNE RONALDSON

### EXECUTIVES IN THE RED

Red Teams are designed to penetrate security in a real world test of effectiveness of security controls, policy, technology and infrastructure. Red Teams view security from an adversary perspective in order to simulate realistic attack scenarios that enable an organisation as a whole to prepare and protect against both simply and sophisticated threats. Red Teams build security culture and provide opportunities for staff to be trained using real world examples. During this presentation we will walk through a Red Team Assessment that simulates a state sponsored attack against one executive, testing the entire security posture of the organisation from a digital, physical, social and supply chain.

### WAYNE RONALDSON BIO

Wayne has conducted security assessments for a range of leading Australian and international organisations. Wayne has unique expertise in Red Team Assessments, Physical, Digital and Social Media Security, and has presented to a number of organisations and government departments on the current and future state of the cyber security landscape in Australia and overseas.

---



## FERNANDO ARNABOLDI



### EMBEDDING DEFENSE IN SERVER-SIDE APPLICATIONS

Applications often rely on secure development practices and third-party defense mechanisms for protection. Whenever an application receives malicious payloads they are either dropped or executed by the affected application. Ignoring these situations aid attackers in performing deep analysis of applications until they are able to exploit existing flaws.

Standards, libraries and third-party defense systems developed to secure applications introduce opportunities for attackers. While some protections have already been implemented in applications and web firewalls, there is a whole spectrum of techniques not being analyzed. This research details how server side applications can incorporate an extensive layer of defense to detect and protect against attackers.

Defense mechanisms will be released in four different languages: .NET, Java, PHP and Python. Throughout the presentation, undisclosed vulnerabilities from secure coding guidelines will be used to exemplify. By implementing the defenses laid out in this paper, attackers may unwittingly become the victims.

### FERNANDO ARNABOLDI BIO

Fernando Arnaboldi is a senior security consultant at IOActive specializing in penetration testing and code reviews on multiple platforms. He has 20 years of development experience in a variety of programming languages and has presented in the past in security conferences such as Black Hat, DEF CON and OWASP AppSec USA.

---



## JOHN DUNLAP

### COMPARISON AND IMPROVEMENTS FOR EXISTING JUMP ORIENTED PROGRAMMING TOOLS

Return Oriented Programming is the go-to method for bypassing modern software memory protections. Mitigations from major hardware and software manufacturers will eventually destroy the viability of this technique. Jump Oriented Programming ("JOP") represents a viable alternative to return oriented programming, that may be more resistant to mitigations. However, tooling has not caught up to Jump Oriented programming. In this talk security researcher John Dunlap will discuss the technique, as well as a comparison of tools used to achieve it. In the talk John will also present his own tools for detecting and analyzing Jump Oriented Programming "gadgets."

### JOHN DUNLAP BIO

John Dunlap is a security Engineer at Gotham Digital Science specializing in static analysis and code review. Gotham Digital science is a boutique penetration testing firm specializing in testing of unusual or otherwise bespoke software systems. John's main research interests include concolic execution, reverse engineering and advanced

exploitation techniques. John has done security research revolving around embedded systems, novel forms of software exploitation and presented at major United States conferences including Defcon, and Derbycon.

---

## PAUL THERIAULT

### IMPROVING PRIVACY ON THE WEB

In this presentation we'll review the current state of web privacy and discuss experimental browser features aimed at improving privacy protections on the web. We'll review one mechanism in particular – “origin attributes” – which provides an extension to the web's regular same-origin policy. Firefox has used this technology to implement the Tor browser's concept of ‘First Party Isolation’ natively rather than the need for a separate build. This technology also allows us to experiment with user-centric privacy features, such as with the Containers feature, which allows users create isolated browsing containers to keep their online identities separate.

This presentation is also call for anyone concerned with privacy to perform their own experiments and contributions. The technology behind Containers is now exposed to Extensions, so that you can build your own features on top of this technology. We'll go through the details of this technology, the benefits and limitations of the mechanism, and run through a sample extension to get you started experimenting.

### PAUL THERIAULT BIO

Paul Theriault runs the security assurance team for Firefox, working to secure both the browser and the Web as an application platform. He has an extensive background in web security, from web app pentesting to contributing to web standards, and as the security lead for the FirefoxOS project.

---

## BRANDON DIXON

### ONE-CLICK BROWSER DEFENSE

When thinking of modern attacks, the web browser is still one of the top delivery vehicles. Whether it's displaying an email or facilitating a link-redirection or merely serving a web page, browsers aid in the attack process. Despite their popularity, many companies focus their efforts defending the operating system, inspecting the network or attempting to keep up with threats through delivered feeds.

In order for any tool to gain adoption, it not only has to be useful, but also needs to easily fit into a user's workflow. Using native browser interfaces, we've created a set of open source browser extensions that not only detect malicious activity, but block it entirely. More importantly, this functionality is delivered in a one-click package and doesn't require any technical knowledge in order to successfully function. Users are able to take advantage of hosted repositories of data or run their own data node and updates are automatic.

This presentation will introduce the browser extension details, highlight how they function and inform users how they could take advantage of this functionality in their organization. Additionally, case studies from successful deployments at enterprise organizations and non-profits will be shared.

No security solution is perfect, but bringing blocking capabilities to the browser without requiring any user change guarantees even the least technical of users can be protected. Originally developed with non-profit and smaller businesses in mind, these security browser extensions can bring peace of mind to any size organization, free of charge.

### BRANDON DIXON BIO

Brandon has spent his career in information security performing analysis, building tools, and refining processes. As VP of Product for RiskIQ, he is responsible for managing the direction of all company offerings. Prior to RiskIQ, Brandon was the co-founder of PassiveTotal (acquired by RiskIQ) where he led development and product direction. Throughout the years, Brandon has developed several public tools, most notably PDF X-RAY, HyperTotal, and NinjaJobs. His research and development on various security topics have gained him accolades from many major security vendors and peers in the industry.

---

## FRASER TWEEDALE

### USER SESSION RECORDING – AN OPEN SOURCE SOLUTION

For Open Source software to conquer the enterprise, we need to play along with government and industry regulations, and help organisations meet their security and audit requirements. Sometimes this means tracking everything a user sees and does. A flexible and scalable Open Source user session recording solution is needed.

In this presentation we will discuss the limitations of existing Open Source approaches, then present the Scribery project, an end-to-end session recording solution with features including:



- terminal session playback and real-time monitoring (including what the user sees)
- centralised storage and correlation with auditd log events
- centralised control of what or whom to record, via SSSD and in the future FreeIPA
- Cockpit integration

The presentation will include a demo of a user session being recorded, stored centrally, inspected and played back.

We will look at the architecture, discuss implementation challenges, and conclude with an overview of the road ahead.

The intended audience is system administrators and security officers responsible for security and compliance, and developers of security, identity and policy management systems.

<https://scribery.github.io>

## FRASER TWEEDALE BIO

Fraser works at Red Hat on the FreeIPA identity management system and Dogtag Certificate System. He’s interested in security, cryptography, functional programming, type theory and theorem proving. Jalapeño aficionado.

---

## STEVE GINTY

### THE MECHANIZED ANALYST

The latest buzzword to make its way into our security community is “AI” (artificial intelligence), also known as “magic.” Companies tout solutions that completely automate people out of the process and simply mark the problem as solved. However, when it comes to analysis work, you need eyes-on-glass humans looking at data to really understand the threats your organization faces. We believe that while you can’t automate the human out of the equation, you can equip him or her with badass tools that make them way more efficient.

In this talk, we will focus on bringing automation to investigations by looking at the relationships between entities on the Internet. Our goal is to demonstrate methodologies—a digital mech suit if you will—that both analysts and machines can apply in order to improve their overall results. We will also include demonstrations of automated capabilities (free and freemium solutions) that attendees can take back to their organisations.

## STEVE GINTY BIO

Steve has more than ten years experience as an information security professional focused on incident response, threat intelligence, and data analysis. As co-founder of PassiveTotal (acquired by RiskIQ), he aimed to advance analysis methodologies and processes to make threat investigations and incident response more efficient and effective. Before joining RiskIQ, Steve spent years researching targeted intrusions against Fortune 500 organisations. His experience includes leading teams of multi-disciplined researchers implementing proactive methodologies to track threat actor infrastructure and malware associated with attack activity.

---

## DR VANESSA TEAGUE & CHRIS CULNAME

### PRIVACY AND BIG DATA

We’ll describe our analysis of open Opal Data, commissioned by Transport NSW. The data treatment used two main methods: first, it broke up trips and journeys and exposed only the total tap-on and tap-off counts at each place and time, with some removal or aggregation of some rare events. Second, it applied a version of Differential Privacy to the totals. We show that it is possible to extract the Differential Privacy parameters, which is not in itself a problem, but rather a further reason for those parameters to be public in the first place. Second, we show that the presence or absence of commuters can be inferred with some (small) probability in some cases.

## DR VANESSA TEAGUE & CHRIS CULNAME BIO

A world expert in the security risks of e-voting, Vanessa has a PhD in cryptography and game theory from Stanford University. Electoral commissions rushing headlong into internet voting tangle with Vanessa at their peril. One of them usually comes out with an egg face – and it’s not Vanessa. Her interest is in cryptographic protocols that support a free and democratic society. She was a member of the team that identified cryptographic weaknesses in the 10% MBS/PBS longitudinal dataset in September 2016.

Dr Chris Culnane is a research fellow in information security in the School of Computing and Information Systems at the University of Melbourne. His research interests include privacy, cyber security and applied cryptography, specialising in cryptographic protocols for electronic voting. He was the technical lead on the Victorian Electoral Commission’s 2014 vVote project, the first end-to-end verifiable voting system to run at a state level anywhere in the world.

More recently he, Dr Vanessa Teague, & Dr Ben Rubinstein, were the team that in September 2016 recovered supplier IDs in the 10% MBS/PBS longitudinal dataset, released by the federal Department of Health. Our results, responsibly disclosed to the relevant Department, immediately preceded the announcement by the Government of the re-identification bill amending the Privacy Act 1988 to criminalise re-identification

---



## MINRUI YAN & MINGGE CAO

### SOME ATTACK SURFACES FOR TELEMATICS HARDWARE

Nowadays, more and more vehicles support the function of telematics, telematics provide convenient experience and support for our users. Through the applications of telematics, they can manipulate the operation of launching vehicles, opening or closing the doors, tracking vehicles and some other capabilities. What behinds the telematics, is a kind of pretty comprehensive and complicated system, which supports the manipulation of the vehicles and the services of vehicle-mounted application. According to some kind of osmotic testing on the components of the telematics system, we found that there is one kind of generalized method which can invade the telematics system. We can access the core network part of telematics easily via this kind of invasive mechanism, and control the whole vehicle through the port.

Meanwhile, we can leverage the vulnerabilities to hijack the data center of the telematics system. So, this kind of threat is very harmful to the vehicles manufactories and merchants. Up to now, we found that this invasive approach is able to impact many vehicles which are in the range of network. This vulnerability is mainly drive by inappropriate design on the hardware structure and improper system security configuration. So, for this presentation, we will show you an example of the idea and method of this invasion, and provide corresponding solution for it to protect the security of network vehicles in the future.

### MINRUI YAN & MINGGE CAO BIO

**Minrui Yan** is a senior security researcher from SkyGo Team of Qihoo360, focused on automotive cybersecurity. He is interested in penetration testing, hardware and developing. Author of Intelligent hardware security. Presenting research on various conferences such as PacSec, POC, CanSecWest, SyScan360, BlackHat Arsenal.

**Mingge Cao** is a senior security researcher of SkyGo Team at Qihoo 360, focused on hardware security. He has being finding several vulnerabilities of vehicle hardware including BOSCH, HiRain, etc. these would affect serval million of the vehicles.