WHAT DO YOU GET WHEN YOU ADD MILITARY POWER, WITH A SPRINKLING OF CAT BURGLAR, AND A PINCH OF TEENAGE TEMPER TANTRUM?

JOSH BURGESS AND CHRIS PIKE
Josh Burgess has more than a decade of cyber threat analysis and mitigation experience serving in multiple positions including in the Intelligence Community, the Department of Defense, as well as the financial sector. In a majority of his roles he has served as the technical lead Threat Intelligence Officer for a large SOC to advise them of the latest threats and ensure a sound security posture. His main role in his current position at CrowdStrike is to support customers by applying his experience in actioning both short-term tactical as well as long-term strategic intelligence data and reporting.
Chris Pike is an experienced intelligence and cybersecurity professional, with over 15 years of experience in the field of military intelligence; with a diverse portfolio of experience covering multiple intelligence disciplines, functions and roles. During his military service Chris worked in a number of cyber operational roles to include leading the MOD CERT threat intelligence team and operating as the lead operational defensive cyber planner. This experience has given Chris a unique insight into the value of cyber threat intelligence and how it can be operationalised to support a mission or business objective.
Intelligence Philosophy
Know thy self,
Know thy enemy
A hundred battles,
A hundred victories

- Sun Tzu
Major problem for the Roman Empire

Utilized deception and misdirection techniques to conquer superior defenses

Move Fast, Move with Purpose, or Fall
Using Deception and Misdirection at Wire Speed
2018 BREAKOUT TIMES

- Russia: 00:18:49
- North Korea: 02:20:14
- China: 04:00:26
- Iran: 05:09:04
- E-Crime: 09:42:23
The Many Faces of Kim Jong Un
THE SPOILED CHILD VERSION OF KIM JONG UN

AFTER THE DEATH OF HIS FATHER KIM JONG UN TAKES CONTROL OF ONE OF THE BEST PROPAGANDA MACHINES EVER SEEN

THE ANNOUNCEMENT OF THE RELEASE OF A SATIRICAL FILM FOCUSED ON THE KJU REGIME

WHOLESALE COMPROMISE OF SONY PICTURES

THEATRE RELEASE CANCELLED
THE BUSINESS VERSION OF KIM JONG UN

PUBLIC ADDRESS ON NATIONAL GOALS

STRIKING SHIFT – ECONOMY FOCUSED

IMPROVE QUALITY OF LIFE

BUILDING YOUR ECONOMY... HOW???
THE MILITARY VERSION OF KIM JONG UN

WHAT DOES THAT LOOK LIKE IN ACTION?

INTERNATIONAL TARGETING OF INDUSTRY VERTICALS IN DPRK 5 YEAR PLAN

WIDE SCALE TARGETING AND COMPROMISE OF FINANCIAL NETWORKS

WANNACRY LEVERAGED AGAINST HUNDREDS OF THOUSANDS OF VICTIMS

INTERNATIONAL TARGETING OF INDUSTRY VERTICALS IN DPRK 5 YEAR PLAN

WIDE SCALE TARGETING AND COMPROMISE OF FINANCIAL NETWORKS

WANNACRY LEVERAGED AGAINST HUNDREDS OF THOUSANDS OF VICTIMS
HIGHLIGHTING RICOCHET CHOLLIMA

LARGELY TARGETING ENTITIES THAT WOULD OPPOSE KJU

DIVERSE SET OF TOOLS SEEN USED AGAINST A SINGLE TARGET

RECENT INTEGRATION OF ANDROID MALWARE

ECONOMIC AND POLITICAL

NATION STATE
HIGHLIGHTING VELVET CHOLLIMA

TARGETING OF ACADEMICS, THINKTANKS AND GOVERNMENT

NONTRADITIONAL GOOGLE CHROME MALWARE

PRINCIPAL OF JUCHE

ECONOMIC AND POLITICAL

NATION STATE
HIGHLIGHTING LABYRINTH AND STARDUST CHOLLIMA

RESPONSIBLE FOR THE WANNACRY OUTBREAK

TOOLSET IS SPECIALIZED TOWARDS THEIR INTENDED VICTIMS

CRYPTOCURRENCY AND FINANCIAL NETWORK TARGETING

NATION STATE

ECONOMIC
WE HAVE DISCUSSED THE PAST, BUT WHAT ABOUT THE FUTURE

ECONOMIC

NATION STATE
Enough with the Scary Stuff... What next?
MOVING FROM REACTIVE TO PROACTIVE

- Enrich everything because *context is KING* without it the 1 might work, the 10 maybe, the 60 Definitely not.

- Behind every intrusion there is a collection requirement understand this and get the resources to build the *correct wall*.

- Adversaries change and adapt TTP’s but there is still a fundamental *consistency* in their attacks.

- The silver bullet is *people*. Effective defense requires dedicated, capable security professionals and knowledge of the threat.
Questions