COMBATTING THE EVOLUTION OF CYBER CRIME

JOSH BURGESS
TECHNICAL LEAD CYBER INTELLIGENCE ADVISOR
Josh Burgess
Americas Threat Intelligence Advisor
Email: Josh.Burgess@crowdstrike.com
Phone: 1-571-432-7004

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.
AGENDA

• Intelligence Philosophy
• The Challenge
• The Consequence
• Speed is Everything
• Knowledge is Everything
• The 800lbs or 362.874kg Gorilla
• Now What???
My Philosophy on Intelligence
Know thy self,
Know thy enemy
A hundred battles,
A hundred victories

– Sun Tzu
The Challenge
How much time do you have... I'll wait...

**CROWDSTRIKE**

**ENERGY SECTOR PROFILE**

**MALECTRUM: ON THE RISE**

- In December 2018, the most popular SANS25 second was the Maelstrom.

**MOBILE INFRASTRUCTURE**

**LAWFUL: SOCIAL ENGAGEMENT**

**LAWFUL: SOCIAL ENGAGEMENT**

The Lawful Bitcoin wallet software works as an alternative to running a proper Bitcoin node. It involves keeping a full copy of the Bitcoin blockchain on the user’s hard drive. As a relatively “light” wallet, it connects to Bitcoin full nodes (or peers) that will validate transactions for them.

In contrast, running Bitcoin Core or another personal client software would involve users validating their own transactions, at a greater computing cost. Bitcoin Core’s lightweight computing footprint, features beyond those of Bitcoin Core, and open-source nature make it the software wallet of choice for...
General Valery Gerasimov published: 
a new methodology in combat 
“preferred way to win.”

- Doctored pictures, Implanted stories, Social Media manipulation, targeted intrusion, misdirection...
- KiberBerkut, Sprut, FancyBears International Hacking Team, Guccifer, CyberCaliphate...

What happens when you don’t know your adversary
Knowing your enemy and their speed
The Spiders
RANSOMWARE IS THE NEW BANKING TROJAN

Wizard Spider Before Ryuk

• Been around since 2016 possibly Dyre since 2014
• Credential Theft and Wire Fraud
• Global targeting at the general public
• Only trusted criminals need apply

OR

Wizard Spider after Ryuk

• Based on the Hermes Ransomware first seen in 2018
• Trickbot is the foothold to gain access
• Waiting until the most opportune time to enable encryption
• Over 100 Million… Yes 100 MILLION in revenue
RYUK AND WIZARD SPIDER AT A GLANCE

Delivered via Emotet or Trickbot

Ransomware is relatively static but the targeting constantly evolves

Netted at 10’s of million dollars in Bitcoin

FINANCIAL

ECRIME
HIGHLY AGILE AND ADAPTIVE RANSOMWARE

SIGNIFICANT SUCCESS ON A GLOBAL SCALE

EXPANDED TARGETING AND NEW TECHNIQUES BEING EMPLOYED

FINANCIAL

ECRIME

GANDCRAB... REVIL... SODINKIBI... PINCHY SPIDER AT A GLANCE
And none of the victims clicked a link

<table>
<thead>
<tr>
<th>TARGET</th>
<th>DATE OF INFECTION</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 Texas cities</td>
<td>16-Aug</td>
<td>$2,500,000</td>
</tr>
<tr>
<td>PerCSoft</td>
<td>24-Aug</td>
<td>Unknown</td>
</tr>
<tr>
<td>Alphabroder</td>
<td>15-Oct</td>
<td>$600,000</td>
</tr>
<tr>
<td>Complete Technology Solutions</td>
<td>25-Nov</td>
<td>$700,000</td>
</tr>
<tr>
<td>Datto RMM</td>
<td>17-Dec</td>
<td>$6,000,000</td>
</tr>
<tr>
<td>Synoptek</td>
<td>27-Dec</td>
<td>$12,000,000</td>
</tr>
<tr>
<td>Albany Airport</td>
<td>10-Jan</td>
<td>$100,000</td>
</tr>
</tbody>
</table>
The Chollimas
KIM JONG UN’S 5 YEAR PLAN

PUBLIC ADDRESS ON NATIONAL GOALS

STRIKING SHIFT – ECONOMY FOCUSED

IMPROVE QUALITY OF LIFE

HOW IS THIS POSSIBLE?
ONE PART SPOILED CHILD, ONE PART BURGLAR, ONE PART MILITARY POWER

TARGETING OF A WIDE RANGE OF VERTICALS

NONTRADITIONAL MALWARE AND USING DESTRUCTIVE AS A SMOKE SCREEN

PRINCIPAL OF JUCHE

NATION STATE

ECONOMIC/POLITICAL
THE WAY FORWARD
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.
- Backup your data and patch
THANK YOU FOR YOUR TIME