ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES

THREAT INTELLIGENCE AND RESEARCH

CHECK POINT SOFTWARE TECHNOLOGIES
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>03</td>
</tr>
<tr>
<td>INVESTIGATION TIMELINE REVIEW</td>
<td>04</td>
</tr>
<tr>
<td>ROCKET KITTEN TOOLS &amp; INFRASTRUCTURE</td>
<td>09</td>
</tr>
<tr>
<td>GEFILTE PHISH—BEST SERVED COLD</td>
<td>11</td>
</tr>
<tr>
<td>WOOLGERED—HOISTED BY THEIR OWN PETARD</td>
<td>18</td>
</tr>
<tr>
<td>REELED IN—PHISHING LOGS ANALYSIS</td>
<td>25</td>
</tr>
<tr>
<td>EPILOGUE</td>
<td>27</td>
</tr>
<tr>
<td>APPENDIX A—INDICATORS OF COMPROMISE</td>
<td>28</td>
</tr>
<tr>
<td>APPENDIX B—MPK TECHNICAL DESCRIPTION</td>
<td>33</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Since early 2014, an attacker group of Iranian origin has been actively targeting persons of interest by means of malware infection, supported by persistent spear phishing campaigns. This cyber-espionage group was dubbed ‘Rocket Kitten,’ and remains active as of this writing, with reported attacks as recent as October 2015.

The Rocket Kitten group and its attacks have been analyzed on numerous occasions by several vendors and security professionals, resulting in various reports describing the group’s method of operation, tools and techniques.

Characterized by relatively unsophisticated technical merit and extensive use of spear phishing, the group targeted individuals and organizations in the Middle East (including targets inside Iran itself), as well as across Europe and in the United States. Many of these targets were successfully compromised by various pieces of custom-written malware; and despite identification and flagging of their infrastructure, the attackers have struck again-and-again by making minor changes to their tools or phishing domains.

Check Point has obtained a complete target listing from the attackers’ servers; among confirmed victims are high ranking defense officials, embassies of various target countries, notable Iran researchers, human rights activists, media and journalists, academic institutions and various scholars, including scientists in the fields of physics and nuclear sciences.

This report provides a summary of the findings including:

- New evidence obtained during Check Point’s independent investigation into attacker infrastructure, including previously unpublished malware indicators.
- Information that appears to reveal the full extent of operations over the past year, and provides unique insight into target profiles and attacker operation internals.
- Analysis of attack data to reveal details on victims and specific industries that may have special significance to Iranian political and military interests.
- Analysis of attacker mistakes that appear to reveal the true identity of the main developer behind the group’s activities (a.k.a. “Wool3n.H4T”), detailed for the first time.

It is our hope this report and measures taken over the past few weeks lead to an effective shutdown of attacker operations (current generation of tools and infrastructure). While Check Point customers are protected against all known variants of this threat, we urge fellow security vendors and malware research professionals to extend malicious IoC (Indicators-of Compromise) coverage in current protection infrastructure.
INVESTIGATION TIMELINE REVIEW
[If you are familiar with previous publications and interested in Check Point’s new insights, you may skip this section.]

The Rocket Kitten campaign/actor group has been studied and analyzed on multiple occasions by different vendors, threat intelligence groups and individual researchers. In a repeating challenge in the malware research domain, we have seen different reports introduce a myriad of code names and operation names for what may very well be the same campaign/actors.

In contrast to malware naming schemes, all reports are in unanimous agreement with strong indications of the campaign’s Iranian origin. This thesis is supported by the individuals and verticals targeted, as part of a plethora of circumstantial and direct evidence. While we should keep in mind digital evidence can be forged and tailored to falsely masquerade as any attacker to deceive a forensic analyst, the overwhelming amount of independent evidence collected over years of attack activity render the notion of a false campaign extremely improbable.

Despite all the reporting and sharing of malicious indicators, Check Point has detected continued active attacks using the same methods and infrastructure. These findings were confirmed by other security vendors, as well as Check Point’s research partners.

It seems as if the attackers, unsophisticated as they are, are completely undeterred by the western security industry’s revelations and publications. Often with the simple replacement of a domain name and minor updates to their malware tools, they continue to carry out their operation undisturbed.

Let us try to review and briefly summarize points of interest from the publications so far.

2 http://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/
3 http://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/
4 https://www.youtube.com/watch?v=WlhhKovlHDJ0
7 https://citizenlab.org/2015/08/iran_two_factor_phishing/
The May 2014 ‘Operation Saffron Rose’ publication identifies an Iranian hacking group formerly named ‘Ajax Security’ (code-named ‘Flying Kitten’ by CrowdStrike) engaged in active spear phishing attacks on Iranian dissidents (those attempting to circumvent government traffic monitoring). This group is potentially linked to more recent Rocket Kitten attacks (different tools, yet very similar mode of operation and phishing domain naming scheme). No concrete evidence of such link has been presented yet.

Newscaster by iSight Partners was released the same month, to detail similar efforts of persistent spear phishing backed by false social media identities pertaining to be journalists of the fake news web site ‘newsonair.org.’ iSight, who reportedly cooperated with the FBI, provides a clear Iranian attribution to these efforts. The report specifies the attackers targeted policymakers, senior military personnel and defense industry organizations in the US, UK and Israel. We did not find direct evidence linking this activity to Rocket Kitten.

ClearSky’s September 2014 blog post first described active attacks using a piece of malware they dubbed ‘Gholee’ (as appears in a malicious payload export function, potentially named after a popular Iranian singer). The researcher points to initial leads into other attacks and notes the threat is currently undetected by the overwhelming majority of AV products.

Gadi & Tillman’s presentation at 31c3 (the 31st Chaos Communication Congress in Germany) was the first clear identification of the Rocket Kitten attacker group, continuing the CrowdStrike naming scheme for Iranian attacker groups. The publication introduced the involvement of hacker persona ‘Wool3n.H4t’ and other identities in forensic evidence obtained from the malicious documents.
The researchers followed to describe two pieces of malware used by the attackers:

- A deeper look into ClearSky’s ‘Gholee’ determined it is the ‘wrapper’ component of an off-the-shelf penetration testing tool originally authored by Argentina-based Core Security. This legitimate PT tool, named ‘Core Impact,’ was illegally repurposed and used for malicious attacks by the Rocket Kitten group.

- A .NET-based credential stealer that pilfers known certain credential storage locations in the infected computer and e-mails them to ‘wool3n.h4t@gmail.com’. This tool appears to be named ‘FireMalv’ by the attackers.

Trend Micro’s March 2015 publication reintroduces the ‘Gholee’ malware (as GHOLE) campaign, and describes ‘Operation Woolen Goldfish,’ as well as an additional ‘CWoolger’—a unsophisticated key-logger apparently named ‘woolger’ (likely a Portmanteau for ‘wool3n keylogger’) written in C++, and present evidence showing its existence starting 2011.

The researchers continue to point at the very likely attribution to the Wool3n.H4T identity as the malware author, whose only online reference was found in an Iranian blogging platform.

In this publication, Trend Micro researchers document Rocket Kitten’s minor update to the Gholee malware (the ‘gholee’ function was renamed to ‘function’), supposedly to avoid the Yara signature published by ClearSky and document the existence of Gholee malware samples dating March 2011, as further evidence for historic attacker activity.

ClearSky continued their investigations into the group’s activities and in June 2015 published a paper dubbing the attack campaign ‘Thamar Reservoir’ named after Dr. Thamar E. Gindin, herself a Rocket Kitten target. ClearSky researchers notably mention the breach of an Israeli academic institution to serve as a hosting service for the phishing web site, and follow to present an OPSEC (operational security) failure by the attackers that allowed ClearSky to learn of a detailed (partial) target list.
This list was analyzed to confirm a strong alignment with nation-state political interests, with specific victims known as adversarial or of intelligence value to Iran. ClearSky also reference an inadvertent public confirmation for the Iranian attribution by the US Department of Treasury in a memo which briefly appeared online, before being deleted.

ClearSky provided many examples of personalized phishing e-mails and communication, including phone calls to victims luring them to open these attachments, demonstrating the group’s persistency and breadth of operations.
The same phishing phone calling scheme was detailed in an August 2015 report by Citizen Lab, describing attempts to lure victims to provide their two-factor authentication tokens. In these attempts, victims receive tailored calls from a person who has clearly researched them, prompting them to take action on received e-mails. Among targeted victims Citizen Lab mention EFF’s Director for International Freedom of Speech Jillian York. The Citizen Lab report describes overlapping phishing domains with ones previously reported, confirming a link with Rocket Kitten.

Interestingly, a special update to the Citizen Lab publication was added to include a response from a news outlet reported to be in close connection with Iranian intelligence, following allegations by exiled Iranian journalist Omid Memarian attributing these attacks to Iranian Revolutionary Guards with ‘no doubt.’ The response mocks the ‘Western Media fishing in muddy waters’ and describe the allegations as ‘weird.’

The latest paper from Trend Micro and ClearSky (dated September 2015) goes a great length to detail the group’s profile and mode of operations so far, and introduces a few more attack incidents, as well as a new ‘downloader’ piece of malware.

---

10 A branch of the Iranian armed forces, sworn to protect the country’s Islamic system and prevent ‘foreign interference’.
ROCKET KITTEN TOOLS & INFRASTRUCTURE
The Rocket Kitten attacker group’s main attack vector is spear-phishing. An effective phishing campaign requires nothing more than a tailored phishing page, hosted on a cheaply-available web server. As described in previous publications, the Rocket Kitten attackers make extensive use of various phishing schemes, often including back-and-forth e-mail correspondence with the victims, or even phone calls to establish legitimacy and reason to open the malicious attachment.

Actual malicious attachments detected in this campaign varied between a set of custom-written malware pieces, or ‘downloader’ components that, in turn, fetch the malware from a remote server and execute in on the victim machine.

Additionally, we have witnessed many attacks using various ‘web hacking’ tools and suites, in attempt to break into victim web sites.

Previously reported custom-malware included:
- **CWoolger**—a C++ based ‘woolen key-logger.’ The malware records all keystrokes and sends out key-log data to a hard-coded FTP server.
- **Wrapper/Gholee**—repurposed Core Impact penetration testing tool. The malware allows a platform for remote access, pivoting for lateral movement and further malware installation.
- **FireMalv**—a .NET based Firefox credential stealer. This tool copies passwords stored in the Firefox browser storage.

Check Point investigations additionally discovered the attackers using the following:
- **.NETWoolger**—a .NET based ‘woolen key-logger.’ This malware is functionally similar to CWoolger. The attackers seem to use them interchangeably, as alternate infection mechanisms (in case one is detected at the victim computer).
- **MPK**—a custom RAT of wider functionality. The malware allows key-logging, as well as remote command execution, screenshot grabbing and traffic monitoring. For a detailed technical description of the MPK malware see Appendix B.

In addition to custom-written malware, we have seen the attackers use various hacking and scanning tools to attack victim web-sites.
- **Metasploit**—An open-source, extensible penetration testing platform. Metasploit’s ‘meterpreter’ payload was wrapped in an executable file and distributed as a RAT attached to phishing emails by the attackers.
- **Havij & SQLMap**—SQL injection tools; Havij originates in Iranian development, while SQLMap is an open source project.
- **Acunetix & Netsparker**—off-the-shelf web vulnerability scanners, attempting to automatically discover and exploit vulnerabilities in common web platforms.
- **WSO Web Shell**—a well-known web shell - PHP script that allows backdoor access on a hacked server. Typically deployed after successful compromise to allow further actions.
- **NIM-Shell**—a web shell of Iranian hacker group origin with similar functionality. Additionally uses Perl scripts on the hacked server.

Web hacking attempts were detected to originate from various IP ranges, occasionally immediately adjacent to known Rocket Kitten C&C servers. We can estimate the attack operators either used these servers directly, or configured them as Proxy/VPN endpoints to channel their attacks.

Combining the research work done so far with observed attacks by Check Point, we can map out a diagram overviewing the attacker’s infrastructure.
• We have no reason to believe any of the mentioned providers are related to the malicious activity. The campaign operators likely masqueraded as a legitimate customer or hacked into the servers without the knowledge of the service provider.
• Specified ranges are likely to be assigned in whole for the attackers use. Due to the dynamic nature of IP assignment, these may expire after the release of this report.
• Because of the way satellite communications work, the infrastructure geo-located to Germany may not be physically located in that country. It would be an educated speculation to assume the servers are physically located in Iran. This assumption is supported by several indicators, including registrant details.
GEFILTE PHISH—BEST SERVED COLD

After learning of an active attack incident from the Rocket Kitten group on a customer network, Check Point researchers decided to actively join the investigation. While the recent paper from Trend Micro and ClearSky (‘The Spy Kittens Are Back: Rocket Kitten 2’) does extensively cover the campaign’s narrative, we aimed to seek confirmation that our analyzed attack was positively connected to the same campaign and set out to provide additional value and insight.

Upon learning of the attack, we attempted to communicate with the phishing web server and gather primary reconnaissance. We learned the same IP address was used for multiple malicious domains. Noting the server on this IP address was alive and well, we decided to probe and question that particular server’s purpose.

What we found took us all by surprise.

We started our web probe by making scripted GET requests attempting to browse to well-known paths. A minute later, we were excited to find a 200 OK response for a few requests, including /xampp and none other than /phpmyadmin(!).

Suspecting false positive results by our scripts, we typed in /xampp into our browser and watched with awe:

![Image 8—A default configuration of XAMPP—on a live attacker server!](image)

We curiously entered the direct path into our web browser and loaded the phpmyadmin interface.

It wasn’t until we actually submitted a query on the server, when we understood that phpmyadmin had been configured to allow password-less root access to any browsing visitor.

“Such a gaping hole must be a decoy” we immediately thought. There is no way nation-state attackers would err in such amateur fashion, leaving their phishing server database exposed... would they?
If only they had paid attention to the ‘XAMPP Security’ page:

Happily browsing through the free-for-all exposed database, we quickly noted numerous schemas; most of them were completely empty (for testing purposes?), with one specific schema standing out: ‘phakeddb’.

‘phakeddb’ contained a set of very interesting tables and data sets; the kind of data sets that fuel the fantasies of malware campaign researchers. Browsing these tables, we found the phishing web application, likely to be a custom development by the Rocket Kitten attackers. The web application would, upon operator instruction, generate the target-specific personalized phishing page for the targeted service (Gmail, YouTube, Hotmail, etc...).

As we later learn, this platform was named ‘Oyun Management System’ by the attackers.
Let us first look at the ‘users’ table:

<table>
<thead>
<tr>
<th>user_id</th>
<th>user_name</th>
<th>user_pass</th>
<th>user_nickname</th>
<th>user_created_date</th>
<th>user_lock</th>
<th>isadmin</th>
<th>pcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>admin</td>
<td>e10adc3949ba59abbe56e057f20f83e3</td>
<td>super admin</td>
<td>2014-08-09</td>
<td>0</td>
<td>✔️</td>
<td>22</td>
</tr>
<tr>
<td>50</td>
<td>anonymous</td>
<td>09266cc9114e778d1945fa0ed04fb</td>
<td>Anonymous</td>
<td>2014-08-09</td>
<td>0</td>
<td>✔️</td>
<td>8</td>
</tr>
<tr>
<td>51</td>
<td>merah</td>
<td>c12c563b4586e36a91dca01a8b00a</td>
<td>mire</td>
<td>2014-08-17</td>
<td>0</td>
<td>✔️</td>
<td>8</td>
</tr>
<tr>
<td>52</td>
<td>124</td>
<td>e87a7a7e424cde4780f43b8c6e92b50cd</td>
<td>razavi</td>
<td>2014-08-17</td>
<td>0</td>
<td>✔️</td>
<td>11</td>
</tr>
<tr>
<td>53</td>
<td>kaveh</td>
<td>46ec41ac034218292950ca51d0f8b9b</td>
<td>kaveh</td>
<td>2014-08-17</td>
<td>0</td>
<td>✔️</td>
<td>18</td>
</tr>
<tr>
<td>54</td>
<td>ahzab</td>
<td>7a9e925c263e831341f247e91211</td>
<td>Ahzab</td>
<td>2014-08-20</td>
<td>0</td>
<td>✔️</td>
<td>40</td>
</tr>
<tr>
<td>55</td>
<td>attache</td>
<td>827ccbe0ea8a706c4c34a16198f4e78b</td>
<td>irakli</td>
<td>2014-08-20</td>
<td>0</td>
<td>✔️</td>
<td>35</td>
</tr>
<tr>
<td>59</td>
<td>amirhosein</td>
<td>e89b359ba900ce11da2be374389e3</td>
<td>ParsAAA</td>
<td>2014-08-21</td>
<td>0</td>
<td>✔️</td>
<td>10</td>
</tr>
<tr>
<td>60</td>
<td>john</td>
<td>e10adc3949ba59abbe56e057f20f83e3</td>
<td>john</td>
<td>2014-08-24</td>
<td>0</td>
<td>✔️</td>
<td>10</td>
</tr>
</tbody>
</table>

The attackers log in to the application, just like any other web platform, in order to set up their phishing campaigns. This server seems to have been deployed August 2014, when all users were created.

And the hash type of passwd fields used? You may not be surprised to learn they used **unsalted MD5 hashes**.

That’s actually not the most oblivious malpractice in this system, however; the hash for the user named “super admin” (assigned with all possible permissions) is `e10adc3949ba59abbe56e057f20f83e3`. Hobbyist cryptographers may recognize this string as the MD5 hash for “123456”.

Looking at user names, we can spot some potentially Persian names or aliases such as merah, kaveh, ahzab or amirhosein. These were potentially the campaign ‘operators’—tasked with social engineering and tailoring a phishing page per target. (hint: “123456” was not the only trivially crackable password in this list)

Moving on to the intriguing ‘conversation’ table, this appears to be an experimental messaging feature between attackers. Unfortunately, it was rarely used.

```
msg_id | msg_id | date          | content                                      | viewed |
------|--------|---------------|----------------------------------------------|--------|
18     | 51     | 2014-09-17    | https://www.youtube.com/watch?v=VZmhdwLdaxw       | 0      |
22     | 54     | 2014-10-01    | file://profiles.google.com/inc.js/0?_schema=1326&m... | 0      |
25     | 54     | 2014-10-05    | file://c4351bd115de77/users.storage.live.com/... | 10     |
26     | 54     | 2014-10-05    | file://accounts.google.com/VA?=C0m3Lu2C2SsegE9QIb2... | 0      |
29     | 51     | 2014-10-29    | Adrese asli: http://outlook.com/owarbu.ac.il red... | 0      |
30     | 51     | 2014-10-29    | http://www.youtube.com/watch?feature=youtu.be&view=S... | 0      |
32     | 51     | 2014-10-29    | Sign in to continue to YouTube                 | 0      |
35     | 51     | 2014-10-29    | please 20 subject for me. tank you attach       | 0      |
34     | 51     | 2014-11-24    | http://profiles.facebook.com/loginuser?_schema=198... | 0      |
```
Most messages include links to various phishing domain pages, perfectly correlating to reported attack pages, proving this database is indeed in direct correlation to the attacks.

Interestingly enough, we can see user id 55 (correlating with the 'attache' username in the users table) making a request:

```
please 20 subject for me.
tank you
attache
```

Later on, user id 60 ('john') pleas:

```
seeyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
We can see template codes for phishing pages, including the descriptive “Victim Full Name,” “Victim User Name” field values. It seems that this application generates the custom phishing templates using these custom fields. Even more telling, we have examples for each field, reintroducing us to our Wool3n.H4T friend [author of keylogger malware by the same group], repeatedly mentioned in this column. This introduces the reasonable possibility that Wool3n.H4T himself wrote this “phishing application” as a supporting tool for the campaign.

There is an intriguing ‘supervisor@ybsoft.com’ reference, too, but ybsoft.com is currently registered to a Chinese electronics shop, so no luck in that direction.

The real jackpot, however, is still ahead.

When we opened the ‘projects’ table, we momentarily lost our breath. A ‘project’ is apparently a single victim [target e-mail address], assigned with a ‘proj_id’, a tasked operator, and the specific link that was generated to be sent to this victim. We just hit 1842 records including all victims attacked starting August 2014 and all the way to August 2015 [when this database was accessed].

Not only do we have the e-mail addresses of all victims, we also have the template values for their respective phishing pages [in the ‘projectmailrequirevalues’ table]!. For example a ‘Google Sign-In’ page normally displays the full name of the victim, as well as a public avatar defined by the user. The attackers had to replicate this look and feel, and filled the database with full names, addresses and photos for every targeted victim.

We verified and retrieved names and images of previously reported victims as expected.
But what does ‘projectlogs’ contain?

Is that what we think it is?

This table contained a log entry for every access to any phishing page, including the credentials provided by the victims, if successfully fooled. We can now use this data to gather insightful analytics on spear phishing activity over one year spanning August 2014 to August 2015. Please see the attack log analysis section in this report.

Continuing our server probe, we discovered a similarly exposed ‘Webalizer’ interface, providing useful analytics including counters and frequently accessed links.
The Webalizer interface neatly presented us with a lot of useful metadata, including “Top 40 visitor IPs” — clearly identifying attacker access to the site, and providing us with many leads for the remainder of the investigation. Interestingly enough, we also found some referrer headers, leading to a path on the same server:

![Image 17—Webalizer statistics for August 2015](image17.png)

![Image 18—login screen](image18.png)
In what can be described as a ‘hacker secret access’ portal—we seem to have reached the web interface of the phishing platform. Testing the ‘admin’ credentials we previously “cracked”—we get:

![Image 19](image19.png)

Image 19—the “Oyun Management System (OMS)” [sic]

We now learn the attackers name this system “Oyun” and actually used Larry Page’s public profile picture as admin’s avatar. The remainder of the interface simply allows access to the phakeddb database, including insertion, editing of “projects” (/targets) and even the internal chat platform as evident in “conversations.”

**WOOLGERED—HOISTED BY THEIR OWN PETARD**

Using credentials hard-coded into the woolen key-logger, we were able to retrieve numerous woolger DAT files [key-logs], as uploaded from victims around the world.

As apparent, the same hard-coded FTP credentials were, in fact, Administrator credentials on the C&C Windows server itself, which had the C$ and D$ NetBIOS/SMB administrative shares openly accessible from the WAN.

![Image 20](image20.png)

Image 20—if you didn’t want to allow researchers to have administrator access to your C&C server

<captain_hindsight.png>

you shouldn’t have hard-coded administrator credentials into your malware.
Among many logged keystroke files containing stolen data, we stumbled on an astonishing discovery: the Rocket Kitten attackers had, in fact, **infected their own workstations**, apparently as ‘test-runs’ for woolger. The attackers failed to remove these files from the C&C server, demonstrating, yet again, utter lack of OPSEC.

Of peculiar interest to us were logs made by none other than ‘Wool3n.H4t’ himself:

![Image 21—The test worked.](image1)

Would you be surprised what followed in the same log file?

![Image 22—The attacker testing his own tool.](image2)

Yes, we actually just witnessed Wool3n.H4T switching through his open windows, including a Microsoft Visual Studio live debugging session of a project called... ‘CWoolger’

In another log, we observe the specific programming of loading of the ‘wsc.vbs’ script, as observed in the Trend Micro publication and others. At this point, there should be no question—we are looking at the malware author’s development workstation.

![Image 23—Mutexes and thread-safety should be the least of your worries.](image3)
The next log shows us the attacker wanted to test whether his tool would accurately capture credentials entered into a Firefox HTTP authentication prompt, and thus he entered his own C&C server...

All of Wool3n.H4T’s retrieved logs were dated October 2014.

Then, we spotted this log segment:

Image 25 – ‘AOL Mail’ already narrowed it
Recorded under the Wool3n.H4T name, a user logs into AOL mail with username ‘yaserbalaghi.’

Could it be the same ‘Yaser’ as noted in the recent Trend Micro and ClearSky paper? (‘D:\Yaser Logers\CWoolger’…) Could it explain the Phakeddb reference to ‘ybsoft’? We don’t know at this point; we have to go deeper.

‘yaserbalaghi@aol.com’ appears to give a technical answer in a long C++ thread in an Iranian programmers forum (‘Barname Nevis’) in Iranian ‘Solar Hijri’ calendar year 1389 (2010-2011):

![Screenshot](image1.png)

The same yaserbalaghi user made several posts, also linking to various programming instructional videos in the subjects of ASP.NET and AJAX, jQuery and SQL injections as instructed by him using screen capture software.

Careful watching of the videos allowed us to learn a few interesting details. For starters, Yaser Balaghi is a Microsoft Visual Studio 2010 user, with familiarity of several tools observed to be used during the ‘Rocket Kitten’ campaign.

![Screenshot](image2.png)

Image 26—Screenshot taken from instructional video by Yaser Balaghi (Engineer Balaghi)
Further inspecting the user names and host names evident in the screen captures, we noticed we were actually in possession of logged keystrokes from an “infected computer” where the user name was “Engineer Balaghi,” strengthening our suspicions. However, we can’t be sure yet; Yaser Balaghi may be a common name or perhaps this is someone related to Wool3n.H4T or the attackers.

A few minutes later, and we spotted this gem of an OPSEC mistake in the SQLi instructional video, which precisely provided the smoking gun we were after:
Wool3n.H4t is caught red-handed. One of his many mistakes, he was now caught giving a public tutorial while logged in under his secret alias, otherwise unlinked with his real identity. These videos were recorded February 2014, prior to the first clear Rocket Kitten attack wave mid-year.

A quick glance on Wool3n.H4t’s desktop reveals a striking match with web hacking attack tools previously described in Rocket Kitten’s arsenal.

Image 29—Havij, Acunetix, Netsparker, SQLMap, wamp, and oh—is that IDA properly licensed?

A few online queries later, we are getting numerous results, cross-referenced to verify as the same Yaser Balaghi, now the main suspect to hold the Wool3n.H4T identity.

Engineer Yaser Balaghi is not only an active member of various programming forums—he had a web site (www.eng-balaghi.com, gone offline since August 2014, still available in the Wayback Machine). In the available archived version of the site he described himself as a “programmer, analyst, consultant and lecturer,” and made himself available for hire.

Image 30—Yaser Balaghi’s stackoverflow account
If all that wasn’t enough, we also managed to retrieve an updated resume for Tehran-based Engineer Balaghi:

Islamic Azad University Computer Software Graduate Balaghi lists his job experience, including “Technical Director and Team Leader of Software Development Team [Private]” (highlighted in original), as well as “Head of Security and Hacking [legal and ethical] [Private]”. Later, he goes as far as listing sample accomplishments and completed projects, including the development and system design for a “Phishing Attacks System” ordered by “a cyber-organization”.

We could go on, but the main lesson of this section can be: if you don’t want people to know you created malware for the government, don’t list it in your CV.
**REELED IN—PHISHING LOGS ANALYSIS**

As reported so far, the attackers persistently e-mailed, called and responded with fake identities, tailored for each victim. The attackers clearly read the public reports about them, respond and adapt their tactics, occasionally showing a creative mindset.

In one reported case, the attacked posed under the true identity of a ClearSky researcher, referencing the recent Rocket Kitten report, attaching “detection software” that does exactly the opposite. This an interesting tactic, worthy of mentioning in social engineering classes. It would be wise at this point to mention that the release of report does not include any accompanying detection or protection tools other than the existing Check Point software blades. If you received this report with an attached executable, it is likely a malicious lure.

In another case, the attackers sent a malicious attachment using the identity of a previously known targeted victim. The Israeli recipient of that attachment was wary enough to suspect the origin of the e-mail and responded with a query: “Is that you or are the Iranians in your computer again?” To which the attackers responded [in perfect non-Google-Translate Hebrew]: “The Iranians will never return to my computer!”

That very well may have been the talk of the day at the Tehran operations center, possibly featured in an email printout in the main dining room.

As the Rocket Kitten group’s behavior was well characterized in previous publications [see the recent report from Trend Micro and ClearSky]. We will focus on new insights based on our analysis of the ‘Oyun’ system victim database. We understand that this database contains a partial view, starting August 2014 to August 2015. While the data can be successfully correlated with logs collected from other servers, we have no visibility of e-mails with malicious attachments (as opposed to phishing links to steal credentials), or any complete web hacking log for attacker activity.

The sheer volume of the target database suggests an extensive operation, the work of a group of people over months. The logs included the visiting IP address geo-located country. Our analysis shows the following distribution:

![Chart 1—Phishing visitors’ country distribution](image)

We have studied the visitor data to determine this includes many attacker accesses to test the site functionality. We know the attackers used addresses from Iran, as well as VPN access from the US, Germany, Saudi Arabia and the Netherlands. The data must be interpreted taking these facts into consideration.
Our primary filtering dismissed around 25% of logs and 15% of projects as ‘test runs’ for the system. The following is based on the remaining seemingly valid entries.

Charting the phishing logs over time, we can observe the following timeline:

We can study this data to make a few interesting observations:

- On average, all phishing pages on this server had 26% success in fooling victims to enter their credentials. These are surprisingly high results, potentially attributed to persistency and well-targeted e-mails.

- On May 26, 2015, there is a unique peak of access to the site, with minimal successes. When analyzed, these accesses appear mostly in 3 batches over periods of minutes, with incremental ‘project_id’s and no data provided, from Israeli IP addresses. We can safely discard these as researcher probes, attempting to ‘brute-force’ phishing pages, immediately preceding the ClearSky June publication.

- The attackers seem to have shut down their platform on June and July (likely due to the publication) and resumed operations during August. We found evidence to suggest the database had been migrated from a previous server.

Slicing the projects table by user_id allows a unique internal look on operator assignment; while our target analysis is far from conclusive, we can share a reserved primary assessment of what each user was tasked with:

<table>
<thead>
<tr>
<th>User</th>
<th>Projects</th>
<th>Target Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>83 projects</td>
<td>strictly system testing</td>
</tr>
<tr>
<td>anonymous</td>
<td>522 projects</td>
<td>this is one of the prominent users in the system, tasked with all around mixed targets—focused on Saudi Arabia, many human rights activists, CEOs and ministry officials.</td>
</tr>
<tr>
<td>merah</td>
<td>147 projects</td>
<td>assigned with all Israeli targets, notably including known physics and nuclear scientists, former military officials, national security and foreign policy researchers. This operator is probably a fluent Hebrew speaker.</td>
</tr>
<tr>
<td>kaveh</td>
<td>57 projects</td>
<td>very little activity—mostly testing and some Venezuelan targets.</td>
</tr>
<tr>
<td>ahzab</td>
<td>691 projects</td>
<td>one of the two busiest operators, in 2014 he targeted a vast amount of Saudi scholars and persons of influence, and later listed education and media outlets in Saudi Arabia.</td>
</tr>
<tr>
<td>124 &amp; attache</td>
<td>233 projects</td>
<td>these users both showed clear targeting of defense sector victims, as well as embassies of Iran’s neighboring countries and others. Quite fitting with one of their usernames, they listed several military attachés in their victim list. Notable targets include representatives from the United Arab Emirates, NATO and other regional posts in Afghanistan as well as Thailand and Turkey.</td>
</tr>
<tr>
<td>john</td>
<td>108 projects</td>
<td>During late 2014 he was directly tasked with Venezuela trade and finance targets, later in 2015 he moved to former Iranians living abroad—listing professors, scientists, journalists and investors</td>
</tr>
</tbody>
</table>

Despite our limited visibility, we can confirm many of these attacks were successful—the attackers gained confidential information from various targets all around the world.
EPILOGUE

We believe the Rocket Kitten case is an interesting case study for the malware research industry, exemplifying a continuing trend in the nation-state attacker profile we have witnessed over the past two years; cyber-espionage is no-longer reserved to organizations with monstrous budgets to hire thousands of cyber-warriors, operate password-cracking super-computer clusters or advanced research to infect your hard-drive firmware. Adversaries will often find simpler ways for effective compromise, such as creative phishing and simple custom malware.

In this case, as in other previously reported cases, it can be assumed that an official body recruited local hackers and diverted them from defacing web sites to targeted espionage at the service of their country. As is often the case with such inexperienced personnel, their limited training reflects in lack of operational security awareness, leaving a myriad of traces to the origin of the attack and their true identities [e.g. Yaser Balaghi, Mehdi Mahdavi and others].

Despite publications, code names and articles in security outlets - the same known attacker group continues to attack with minimal interruption.

Highlighting a repeating industry problem, minimal changes to existing malware often evade most current protection solutions. Effectively stopping attackers must involve action on top of analysis efforts.

We approached and will continue to approach hosting providers through the assistance of CERT coordination and other bodies in various countries. We hope these efforts are fruitful, and can help disable or reduce the attacking infrastructure.

If you would like to share important information regarding this campaign, please use icanhazrocket@checkpoint.com
APPENDIX A—INDICATORS OF COMPROMISE

**Samples**

All hashes are MD5 or SHA1

### Lure Documents / Droppers

<table>
<thead>
<tr>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>01c9cebbc39e273ac1f5af8b629a7327</td>
</tr>
<tr>
<td>08273c8a8735925ae1563543af3715c</td>
</tr>
<tr>
<td>1685ba9dadb0e136d68e0b1a80a969b5</td>
</tr>
<tr>
<td>177ef7faab368857240373017ff9c4</td>
</tr>
<tr>
<td>1ceca1757cb652ba7e5bd045f2038955</td>
</tr>
<tr>
<td>266cfe75aa0a66776df9fd8cd2fee1f1</td>
</tr>
<tr>
<td>271a5f526a638a9ae712e6a5a64f3106</td>
</tr>
<tr>
<td>2cb23916ca60a63a67d974f4ddebeb2a11</td>
</tr>
<tr>
<td>393bd2fd420eeef2d4ca9d61df759f0c</td>
</tr>
<tr>
<td>3954f1588e273ab5743db56a81051b</td>
</tr>
<tr>
<td>48573a150562c577422203583456b4c02</td>
</tr>
<tr>
<td>4bf221e8b068385ca1bffe8fd609c0104</td>
</tr>
<tr>
<td>50d3f1708293f40a2c0c1f151cc2c426f</td>
</tr>
<tr>
<td>54ee3ebebfeed79d4ddfffd1423df5f5e28</td>
</tr>
<tr>
<td>55ff220e38556ff902528ac984f72dc</td>
</tr>
<tr>
<td>5a0990d0c5ecacac1407fb32ee1c8172</td>
</tr>
<tr>
<td>5af0c8b3c6f8ed4fd1a3f68961f5452</td>
</tr>
<tr>
<td>60f5bc820cf387eb51ele20fed290b5</td>
</tr>
<tr>
<td>61a808e0b645c4824d79865be888ed</td>
</tr>
<tr>
<td>85b79953fb2b33fb6118dc04e4c30910</td>
</tr>
<tr>
<td>8ed01ac79680d84c0ee7a5f027d88b8a</td>
</tr>
<tr>
<td>9fc345c25e6ab94ca2db6ee95d2c861</td>
</tr>
<tr>
<td>ac94ee83c91a784a88ff26cf85e727a</td>
</tr>
<tr>
<td>aeb9d12ecebe73bfa91616ebacf24831b</td>
</tr>
<tr>
<td>c9ea312c35e9ac0809f1c76044929ff2f</td>
</tr>
<tr>
<td>d0c3f4c98964d1a7c42737134ffbc4ce2</td>
</tr>
<tr>
<td>d14b3e0b82e3b5d6b9c69b9f8f8126d</td>
</tr>
<tr>
<td>e1a5b4ffe612270425d5d31f4c336aa9</td>
</tr>
<tr>
<td>f68a0a3784a7edf60ad9333ec209cbf</td>
</tr>
<tr>
<td>f8547010e4b238f8feb76f4e8a7563e6d</td>
</tr>
<tr>
<td>0828cf2e332918456b9c978a9590781095b2b53</td>
</tr>
<tr>
<td>0f4fbfd89d080ed319597754e63930f8eccc49b0</td>
</tr>
<tr>
<td>0a99a131144afe8c8b731e6bb842a4f38101ac5</td>
</tr>
<tr>
<td>2627c03234275e64f1f39597a352573e45c0f1e</td>
</tr>
<tr>
<td>20e3643e41930bafef248b71974659543a3d774</td>
</tr>
<tr>
<td>46a995df8d9918ca0793401109f04796adcb9f</td>
</tr>
<tr>
<td>4711f063a0c67fb11c05efdb4042477799efafaf</td>
</tr>
<tr>
<td>476489f75fed479f19bac02c79ce1bebc62a6633</td>
</tr>
<tr>
<td>64b1a30e627dd85c8d5634e769d239080e6f8dd</td>
</tr>
<tr>
<td>6571f29a0aee8f45899b256458da78ac51e6bb</td>
</tr>
<tr>
<td>788d81f3bclc02e685a988d8405f375c0ac2162</td>
</tr>
<tr>
<td>9579e653aeef03ff7d362e0569bece07a8b1b3</td>
</tr>
<tr>
<td>a9245de692c16f90747388c09e902c3ee34577e</td>
</tr>
<tr>
<td>ad6c9b003285e01f6ca02148917ec78c7d751</td>
</tr>
<tr>
<td>ae18bb317090e16f765ba2e88c3d72d648db2798</td>
</tr>
<tr>
<td>b67572a18282e79974d61fffb8ca3d0ff4c1a0b</td>
</tr>
<tr>
<td>c485b5d95283d7a1ac80380080d7774db9d8248</td>
</tr>
<tr>
<td>c727b8c43943986a888a0428ae7161ff001bf603</td>
</tr>
</tbody>
</table>
FireMalv Credential Stealer
0b0e2c4789b895e8ac44b6da284aecl
29d93b156bcfbccecf79c5ba389047961a1ba76ee

Woolen-Keylogger
0a22323c1d5add9d7aabdf630b6ed5af
0e2dc1cb6da45d68ee9c751e37df73b
1a2b18cb40d82cc79eb2ef923c3abd0
1f768865c272d5205f9070c2541a68c
3c6c1722acfb70bfa4453b69e99c98bb
662d094799e9c7108f35c00eb894205f
b4790618672197cab31681994bbc10a4
c72dce99e892bbf2537f5285a01985c0
f7e093d72d2616ecb9067934af15f70
f898eef9da0482ob2b7f9e063645a7
f9b235067b1c607b5b26896d465b6665
2996b0c4157f226761073333ff2e82b588ddfe8e
5d334e0cb4ff58859e91f9e7f1c451ffdc7544c3
8e1bd64acdbbe819ac60650eb1fa4f51f330ec
af2flad2360333baed22d5f9354c4fc3820c475
a56b39d3919f15649106a039469013479a31ba4b
b9842058c88170cc45183aaaee4206c74e6c7351
c8096078f06c3fbb6d82c5b00211802168f9cba
d55b2b30fe2d4759c199e3659d561a50f88a7f2be
d2b8f49b4e76c2f538a3a6b222c35547c802cefe
eh66e663b2fa980c6b228fc2e04304ce8992401d
fafa0fe422259d36494a0b2c9ccef40dee978f31
Network Traffic

Wrapper/Gholee
HTTP/HTTPS [80/443]
index.php/?c=\w+&r=\d+

Woolger

MPK
raw [8900,8899,8987,9090,1993] -
\\\\[mpk\\]\\d{4} example: //\[mpk\\]2012
\\\\[smpk\\]\\d{4} example: //\[smpk\\]1992

Domains
account.login.gfimail.us
accounts.google.uk.to
account-user.com
drive-google.co
drives-google.co
gfimail.us
gmail-member.us.to
goog\le-setting.com
goog\le-verify.com
login.miicrosoftonline.us.to
login.office365.uk.to
logins-verify.com
login-users.com
mail.mail2.mod.gov.af.mail.al
mail-verify.com
my.idc.ac.il.my.to
outlook.profile.com.hmail.us
outlook.tau.ac.il.mail.al
owa.inss.mises.org.il
owas.haifa.ac.il.info.gf
owas.haifa.us.to
profile.gmail.us.to
profile.google.uk.to
profiles.faceboek.in
profiles.googel.com.inc.gs
profiles.googlemembers.com.home.kg
profiles.google.uk.to
google.co
secure.www.cfr.us.to
service-logins.com
signin-users.com
signin-verify.com
signs-service.com
verification.google-it.info
video.google.co
webmail.tau.ac.il.us.to
webmail.technion.ac.il.us.to
yahoo-profiles.uk.to
youtube.com.now.im

**IP addresses**

[107.6.181.96-127]
[107.6.172.50-62]
[107.6.154.224-231]
107.6.181.116
107.6.172.54
107.6.172.55
107.6.181.114
107.6.172.51
107.6.172.53
107.6.181.100
107.6.172.52
107.6.154.230
5.39.223.227
31.192.105.10
[5.145.151.1-7]
5.145.151.6
[84.11.146.52-63]
84.11.146.55
84.11.146.62
84.11.146.61
[109.169.22.69-72]
[109.169.61.4-8]
109.169.61.8
109.169.22.69
109.169.22.71
109.169.22.72
162.223.90.148
162.223.91.226
162.222.194.51
212.118.118.100
APPENDIX B—MPK TECHNICAL DESCRIPTION

The malware appears to be named 'MPK' by the attackers. This may be related to "Masoud_PK" as witnessed in the Iranian blogging web-site under the wool3n.h4t blog name.

Installation

For persistence, the malware will add itself to autorun under an "explorer" entry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The malware includes a Visual Basic script ('tmp.vbs') script, which will try to initially copy the malware executable to its destination:

Sub CopyFile(SourceFile, DestinationFile)
    Set fso = CreateObject("Scripting.FileSystemObject")
    Dim wasReadOnly
    wasReadOnly = False
    If fso.FileExists(DestinationFile) Then
        If fso.GetFile(DestinationFile).Attributes And 1 Then
            wasReadOnly = True
        End If
        fso.DeleteFile DestinationFile, True
    End If
    fso.CopyFile SourceFile, DestinationFile, True
    If wasReadOnly Then
    End If
    Set fso = Nothing
End Sub

copyme = WScript.Arguments.Item(0)
copyto = WScript.Arguments.Item(1)
CopyFile copyme,copyto,0

Also, it will execute the following WScript, which will start the malware itself after exactly 9 seconds.

WScript.Sleep 9000
CreateObject("WScript.Shell").Run "iexplorer.exe [1]"

Main operation

This malware is basically a RAT (Remote Access Trojan). It implements such functionality as a key-logger, sniffing TCP and UDP traffic, taking screenshots, as well as a remote command shell.

Also, it may gather a lot of information about the target system such as enumeration of files, drives, services, process information and the ability to send any file to the C&C server.
Less important, but still sensible information may be exfiltrated:

- Primary display resolution
- Has administrator rights or not
- Processor information
- Hostname information
- Windows version
- Service Pack version
- Amount of memory installed on the target system
- Network adapters and network configuration information
- TCP connections table

The following mutex will be created:

```
[2]opened
```

Then, the malware will check if the following mutex exists:

```
MyApp1.0
```

If it does, the malware will exit, so only one instance of the malware is allowed at a time. If not, it will continue to the main operation.

**Keylogger**

Keylogger stores keystrokes to the following file:

```
%TEMP%\log%d.txt
```

Here is a sample of malware key-log output:

```
(((((((Hello new File))))))))
+++++++++++++
Window= VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark
+++++++++++++
[UP] [DOWN] [UP] [UP] [DOWN] [UP] [UP] [DOWN] [UP] [UP] [DOWN] [UP] [UP] [DOWN] [UP] [UP] [UP] [DOWN] [DOWN] [DOWN] r
+++++++++++++
Window= Command Prompt
+++++++++++++
cmd[ENTER]
+++++++++++++
Window= C:\WINDOWS\system32\cmd.exe
+++++++++++++
notepad[ENTER]
+++++++++++++
Window= VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark
+++++++++++++
[DOWN] [UP]
+++++++++++++
Window= Untitled - Notepad
+++++++++++++
test test test
+++++++++++++
```
This file will be sent to remote C&C server later on.

If the malware detects an open "Gmail", "Yahoo" or "Outlook" window, it will add special processing so the attacker can easily recognize the data that is the most valuable to him. The following string will be appended to the output file:

```
\\r\\n\\nMail Find
```

**Webcam capture**
The malware may capture photos from an attached webcam. Files are first saved with the name test.bmp, later converted to JPEG and saved under the new file name Cam.jpg, eventually exfiltrated to the C&C server.

**TCP Connection Table**
The malware will gather available metadata regarding current TCP connections using the GetTcpTable API, and send a formatted version of the obtained data to the C&C server.

**Screenshots**
The malware may take screenshots. The filename used for screenshots is Screeny.jpeg.

**Remote Shell (Live Command Execution)**
The malware creates the following process as a live command prompt:

```
cmd.exe /c cmd.exe
```

This process' output and input are attached and redirected via pipes to the remote C&C server, allowing the operator to type in commands to control the victim computer. The following line is first sent to the server:

```
Welcome To mpkshell Command Line (This Message Send From Server)
```

**Traffic Monitoring**
The malware may sniff all TCP and UDP traffic on the machine. This is achieved through the use of RAW sockets. The following status strings can be sent to the C&C server:

```
Initializing Winsock 2.2...
Creating RAW socket...
Configuring socket for packet interception
Starting the sniffing process...

UDP Packet Information:
Source IP: %s DESTINATION IP: %s
SOURCE PORT: %d DESTINATION PORT: %d
PACKET DATA:

#############################################################

TCP Packet Information:
Source IP: %s DESTINATION IP: %s
SOURCE PORT: %d DESTINATION PORT: %d

#############################################################
```
If the current user privileges are insufficient for such action, the following error is presented:

```
the processs is not admin try after restart to while mpkProcess To Admin...
```

**File Exfiltration**
The malware may exfiltrate any file to the remote C&C server. The malware also contains the ability to enumerate all files on the system or find a specific file with the required filename specified by the operator.

Upon file exfiltration, the file is checked for size. This is performed in order to send the file in 4Kb ‘chunks’, where each chunk frame is sized 0x1014h bytes.

Before uploading any file to the C&C server, the malware will report its size:

```
length: %d
```

After sending each chunk, the malware will report the current transfer status:

```
%d Bytes / %d Bytes
```

When the transfer will be finished, it will report completion using the following string:

```
Completed: %d Bytes Downloaded.
```

If there was any problem, this string will be reported:

```
Failed to open %s, %s not found.
```

**Communication protocol**
The malware uses raw sockets over IP protocol (IPPROTO_IP flag), effectively implementing its own protocol for data transfer.

The executable’s own “File Version Info” is parsed to retrieve the server IP, trivially encoded into the “Company” value:
This data contains hardcoded IP address and port of C&C server. In this sample it is:

83.170.33.67:9090

A connection will be established to that IP, while sending periodic 'keep-alive' messages, containing these 6 bytes:

123456

File-exfiltration packets are 0x1014h bytes long. The first 2 bytes indicate the type of file to be exfiltrated:

- 0811h—logs (initial packet)
- 0810h—logs (subsequent packets)
- 080Fh—logs (final packet)
- 0BCDh—webcam images (initial packet)
- 0BCFh—webcam images (subsequent packets)
- 0BCEh—webcam images (final packet)
- 0803h—screenshots (initial packet)
- 0805h—screenshots (subsequent packets)
- 0804h—screenshots (final packet)
- 13C2h—error with file

The filename is located at offset 0x08h of the first packet. Subsequent packets include file contents only.
The Check Point Incident Response Team is available to investigate and resolve complex security events that span from malware events, intrusions or denial of service attacks.

The team is available 24x7x365 by contacting emergency-response@checkpoint.com or calling 866-923-0907