The Spy Kittens Are Back: Rocket Kitten 2

Cedric Pernet
(Trend Micro Cybersafety Solutions Team)

Eyal Sela
(ClearSky Research Team)

A **TrendLabs**SM Research Paper

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

Building on the Trend Micro paper released this March on Operation Woolen-Goldfish [1] and the ClearSky research on GHOLE malware [2] (September 2014) and Thamar Reservoir [3], we continued our efforts to monitor this particular group of threat actors to see if any of their movements have changed. Trend Micro and ClearSky continued monitoring Rocket Kitten for the past months and decided to join forces to release this paper. With new attack cases that show the different tactics and techniques that Rocket Kitten uses, we want to shed further light on the group's dealings and come closer to understanding their motivations and goals and who they may be representing.

Our findings show that Rocket Kitten is still active, retains a growing level of persistence, and acts ever more aggressively in terms of attack method. We also found that recent publications on the group's activity have done nothing to change their behavior or reduce their activity. They don't seem to bother to have to "disappear." With this paper, we feel fairly certain that Rocket Kitten's prime targets are not companies and political organizations as entire bodies but individuals that operate in strategically interesting fields such as diplomacy, foreign policy research, and defense-related businesses. We believe the espionage factor and political context make their attacks unique and very different from traditional targeted attacks.

SECTION I

Targeted attacks and cyber espionage

Targeted attacks and cyber espionage

The greatest source of risk in cyberspace emanates from groups with the resources and commitment to relentlessly target a company, a government agency, an organization, or even an individual until they succeed in breaking in and taking what the victim values most. This usually involves an unauthorized person gaining access to a network and staying there undetected for a long period of time via a targeted attack. Typically, the purpose of a targeted attack is to monitor target systems and exfiltrate data from these, as opposed to causing damage or disruption. Therefore, there is an innate connection between traditional espionage and targeted attacks. One can say that a targeted attack evolved from the tradecraft of espionage. The difficulty very often lies in detecting targeted attacks in a timely manner and even more in pinpointing attackers' identities and their financial backers, understanding their motivations, and where the attacks are coming from.

This is also the case when it comes to political espionage carried out in the cyberrealm. Any espionage activity does not usually go after monetary gain and it is very difficult to attribute it to a certain group or nation-state. The attackers can be anything from self-anointed cyber units with a political cause to cyber-capable separatist groups, state-sponsored hackers, or actual covert intelligence agents. Many times, such instances of cyber espionage are attributed to nation-states because they are the most likely to have the greatest motivation, they have the most to gain, and they are most capable of funding and maintaining cyber-espionage efforts without being detected.

When we look at the Rocket Kitten case, we are not dealing with cybercriminals that conduct corporate espionage to obtain access to sensitive documents or resell confidential information and intellectual property. This is an obvious case of politically inspired or motivated espionage.

SECTION 2

Rocket Kitten: Persistent spies

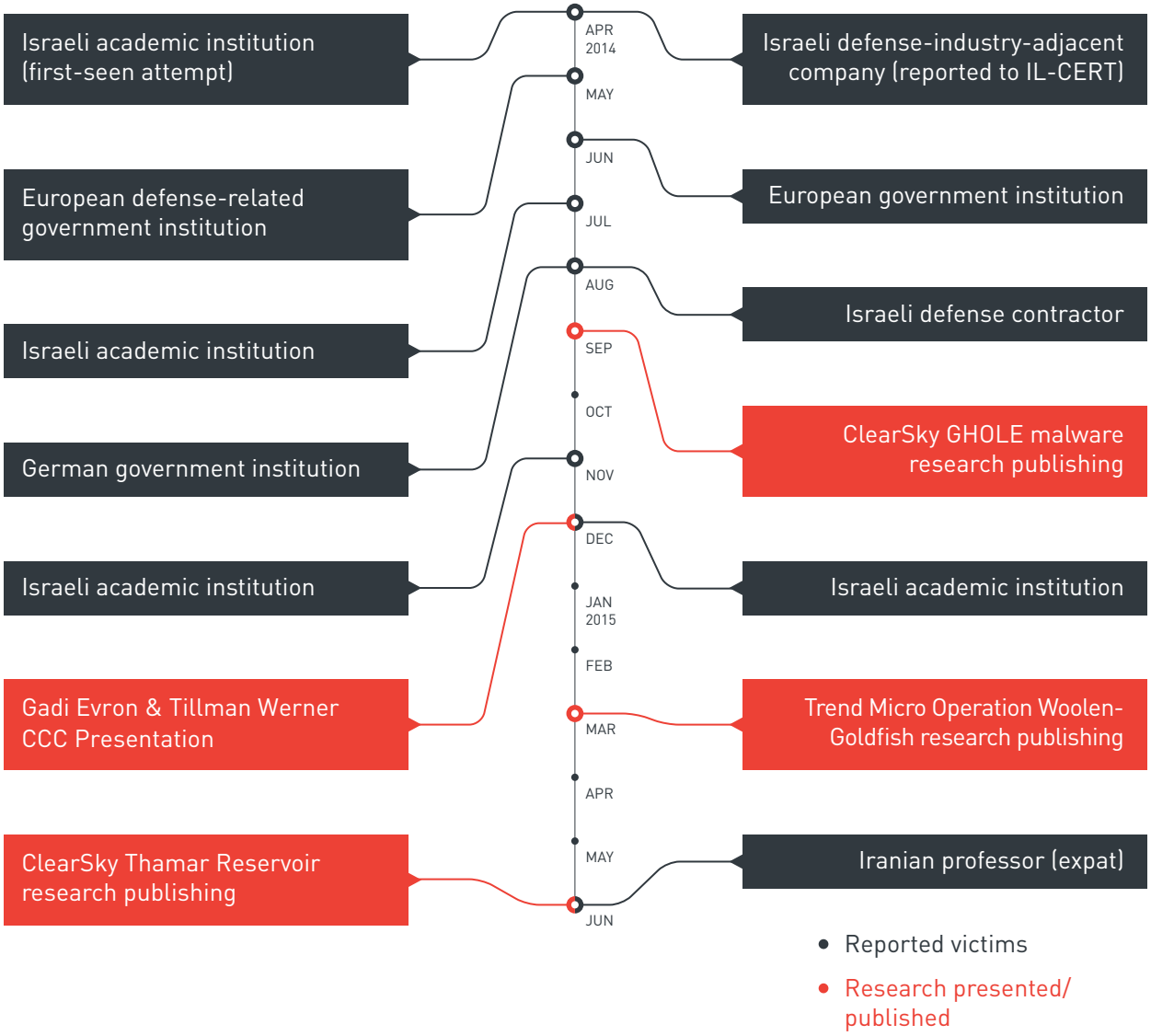
Rocket Kitten: Persistent spies

Attacker profile

Since mid-2014, a group of attackers was observed by different computer security professionals, including Trend Micro and ClearSky. We have documented some of their moves. The set of targeted attack campaigns have been dubbed "Rocket Kitten" and the perpetrators as the "Rocket Kitten Group." Additional sources indicate that the group may have been active as early as 2011 and increased their activities in 2014.

ClearSky first monitored attacks that involved GHOLE—a malicious version of the Core Impact Pro® penetration-testing tool. Core Impact Pro is a legitimate commercial security product that, being a powerful investigative security tool, also bears some potential for misuse with malicious purposes. It is executed by a malicious Microsoft® Office macro. Following ClearSky's research, Gadi Evron and Tillmann Werner, in a presentation at the Chaos Communication Congress (CCC), reported attacks conducted with the same malware that according to them very strongly pointed to nation-state origin [4]. This March, Trend Micro published a paper on Operation Woolen-Goldfish, which targeted a number of European businesses and organizations via spear phishing [5]. This finding showed a connection to the Rocket Kitten campaign seen in December 2014. The Trend Micro paper also showed the use of a new exclusive piece of malware that threat actors called "CWoolger."

Just this June, ClearSky detected new movements from the group, which showed an attack intensity that exceeded our estimations by far. ClearSky has learned of 550 targets, most of which are located in the Middle East. It documented some findings in "Thamar Reservoir [6]." In this paper, Trend Micro and ClearSky combined research results to shed further light on Rocket Kitten's tactics and methods, and show that the focus right now is very much on individuals rather than on organizations.

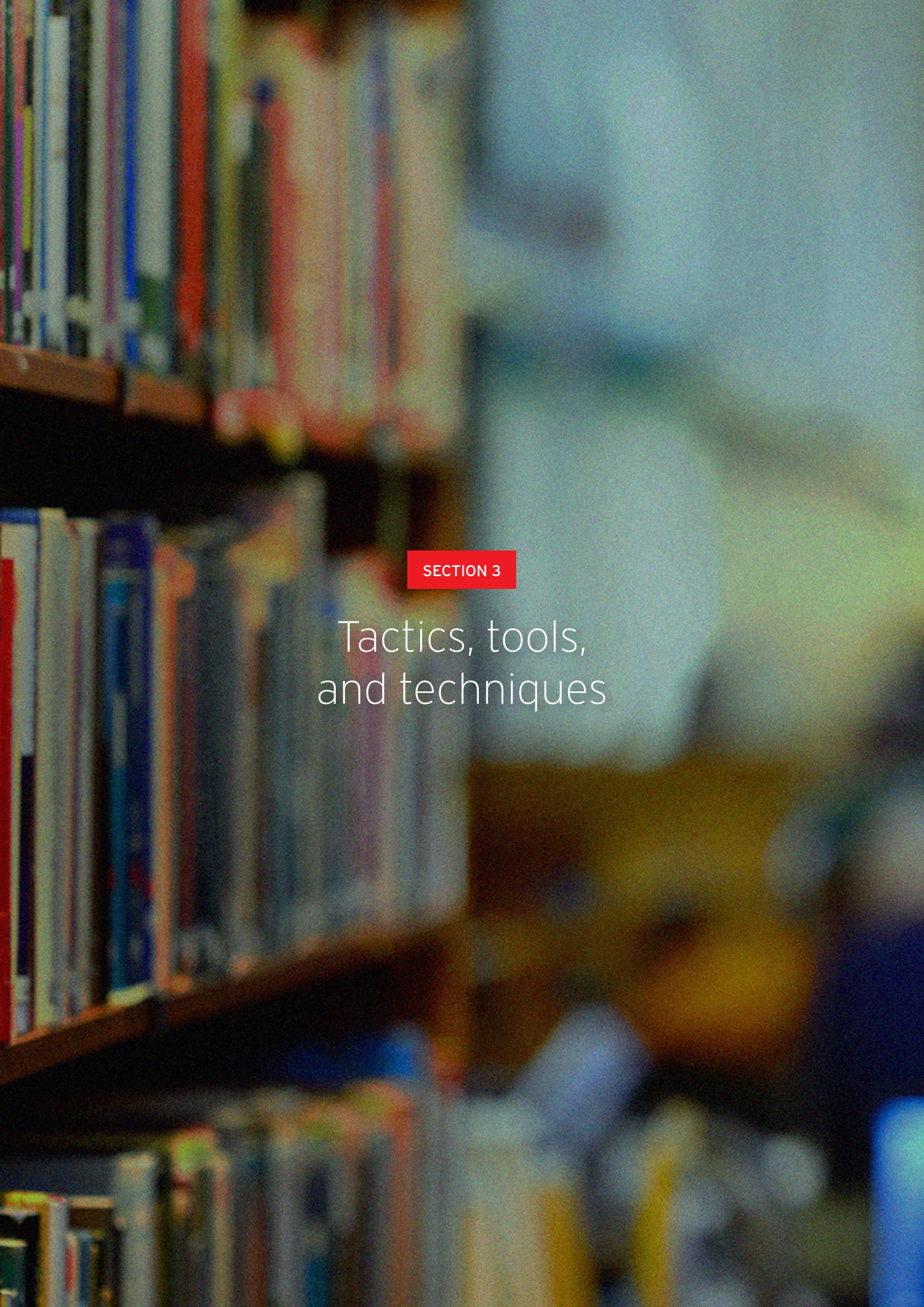


Timeline of Rocket Kitten-related activities

What is Rocket Kitten after?

From our monitoring efforts, our analysis of the attack setup, and the type of people targeted by the threat actors, we drew the conclusion that Rocket Kitten mainly targets different verticals in the Middle East. Their favorite targets seem to be involved in policy research, diplomacy, all aspects of international affairs, defense, security, journalism, human rights, and others. We also observed attacks targeting organizations located in Europe but in the bigger scheme of things this activity is marginal (about 5% of the total number of targeted attacks). The actors do not seem to be motivated by a hacktivist agenda. To us, it is not at all clear what kind of specific information Rocket Kitten is generally after but it is clear that it has to do with espionage.

As we have not seen what documents or information the actors typically look for when they obtain access to a computer or what were exfiltrated following a compromise, it is hard to speculate. From the facts that we have, we can only assume what their motivation and goal may be, no evidence can support any attribution we would claim at this point. What we know is that the individuals targeted often had strategically interesting professions from a political or geostrategic perspective. They are scientists, journalists, researchers, and sometimes expatriated Iranians living in Western countries. These facts suggest that Rocket Kitten may be engaging some sort of foreign political espionage campaign and may want to find regime-opponents active in driving policy in different ways. There are state actors in the region who are interested in gaining access to the information that can be found in people's computers and emails. These people are professionally affiliated with the foreign policy and defense sectors and there is an interest in finding out who they are talking to and what kinds of action they support.



SECTION 3

Tactics, tools, and techniques

Tactics, tools, and techniques

Strategy and standard operating procedure

As in any typical targeted attack, Rocket Kitten utilizes several different malware types and has a concrete tactical setup to compromise an individual or an entity. This compromise seems to mainly serve the purpose of monitoring communications and extracting information, in short, espionage. The victim may be the desired target because the information he holds is valuable to the attacker but he may also just be a stepping stone to reach the actual target.

Rocket Kitten's operating template, which remains constant in almost every case we have seen, has the following components:

1. **Point of entry:** Rocket Kitten uses spear phishing and social engineering to establish contact with either the primary or secondary victim. This can be done by faking accounts and identities:

    - Using fake Google Drive™ or Gmail™ accounts (The Rocket Kitten Group often impersonated persons of interest and public figures such as Israeli engineers.)
    - Using stolen documents that suggest a legitimate cause and sender
    - Using social media accounts as in Facebook to directly contact targets, create rapport via private messages, and log correspondence as well as consequently make users visit phishing websites

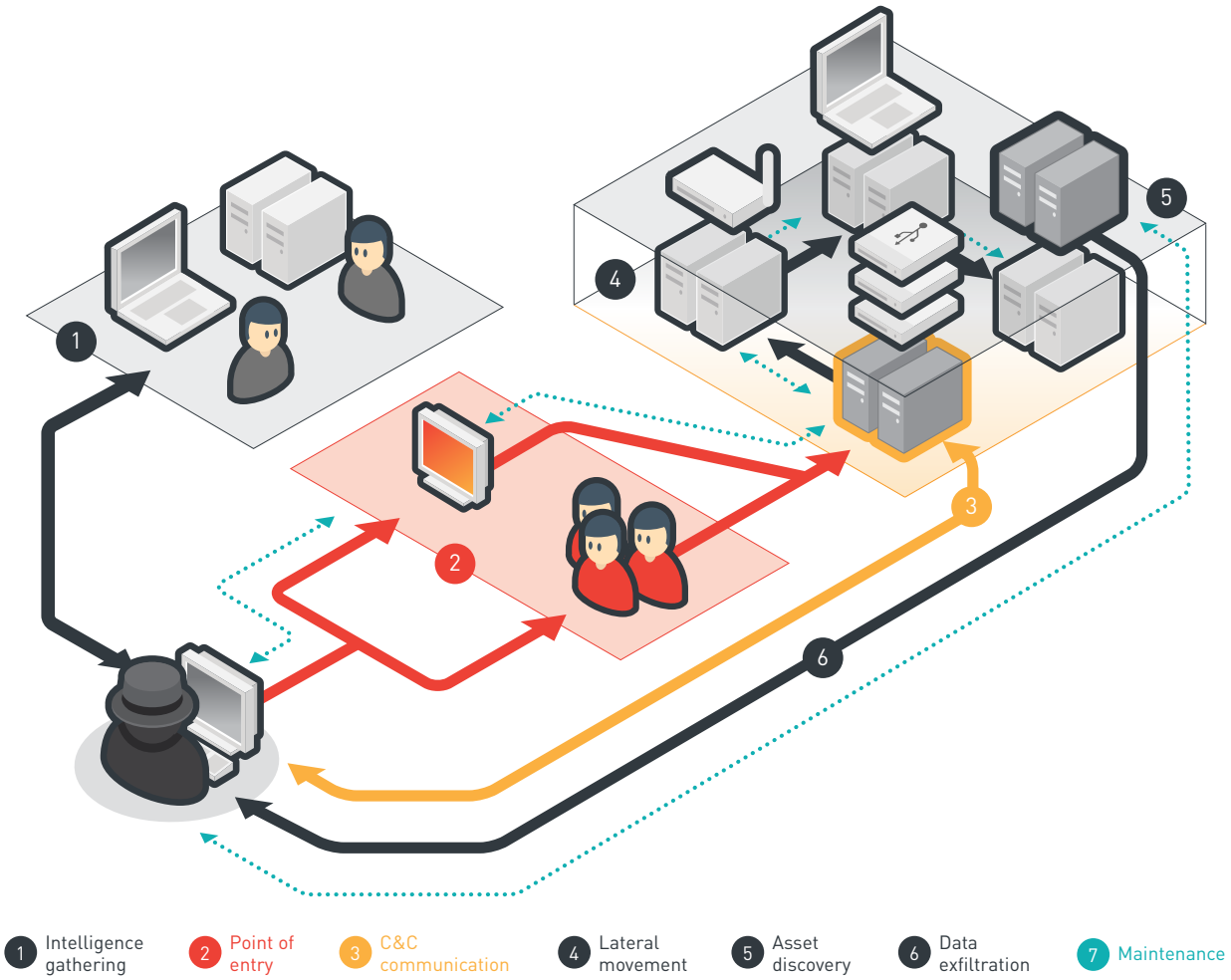
    The spear-phishing email contains a link or a file that when clicked or opened unleashes a payload that takes over the target machine.

2. **Command-and-control (C&C) communication:** The infected computer communicates with a C&C server. It can download whatever malware is available or intended for the cause and purpose of the attack.

As soon as the actors get the user's password (through a request to type it sent via an email, a Facebook message, or a phone call), they take over the chosen account right away and any other accounts they can get their hands on (Facebook, other email accounts, and cloud accounts). They can employ a keylogger (detected by Trend Micro as TSPY_WOOLERG [7]) that logs keystrokes.

They can, for example, connect an application to your Gmail account (in the cases we've seen, Microsoft Outlook® obtained access to the Gmail account as a "connected app") so we assume that the attackers downloaded all of their victims' emails for offline processing.

They can also install any other piece of malware.



Rocket Kitten attack components

Simple tools and lack of professionalism

The Rocket Kitten Group uses both relatively simple tools that we suspect they developed as well as more advanced, publicly available ones, which may have been either purchased or stolen. What strikes us about the attackers is that they don't seem to put much effort into quality assurance when it came to content—how emails and phishing pages are formulated—and so, make a lot of mistakes (typos and grammatical errors). This, of course, makes patterns relatively easy to identify once we know what to look for. However, the attackers do make up for these disadvantages with persistence. Based on our research and profiling, we believe the members of the Rocket Kitten Group could be former cybercriminals who ventured into a new field for some unclear reason and so use some of the methods they used to. Many of their techniques are typically observed in criminal endeavors.

Persistence

The most notable Rocket Kitten strategy lies in numerous attempts to attack the same (chosen) targets for as long as necessary, even if that means trying on a daily basis and with ever new cover stories and convincing techniques to entice users. The idea is to barrage targets until they eventually slip and inadvertently allow the attackers to obtain the desired information, whether primary or secondary in nature—directly stealing credentials from or taking control of victims' computers. Often, even if targets are aware of impending or already-occurring attacks (when they receive malicious messages on a daily basis or are repeatedly requested to reset their passwords), it is almost impossible to defend against attempts, making professional guidance indispensable. The attackers try to overwhelm targets by executing numerous password-reset attempts, making victims believe they are losing control over their accounts.

Work versus private accounts and devices

The Rocket Kitten Group prefers to go after victims' private email addresses and other accounts rather than their organizational ones. This is a clever move, taking advantage of their lack of peripheral protection at home as opposed to in an organizational setting where monitoring systems are in place and security personnel can help as soon as alarms go off. Now, the attackers very well know that while in theory, work and private lives are completely separate; in the real world, people use personal cloud services (Gmail, Google Drive, Yahoo!®, etc.) and personal devices (home computers) to store and share work-related content. What this constellation creates for the attackers is a blissful chain reaction. First, they can gain access to professional, work-related information by attacking and infecting unprotected, nonorganizational access points. By extension, they are also able to use now-infected personal devices or accounts to breach organizational computers and networks.

Infection vectors and malicious applications

Social engineering and spear phishing

Rocket Kitten primarily infects systems via spear phishing. They send spear-phishing emails, sometimes paired with social engineering techniques, to targets. They basically rely on psychological manipulation in order to convince targets that they are who they claim to be. As an added layer—to make emails even more credible—they use stolen documents that in the victims' mind should "prove" their identity and mission.

Rocket Kitten targets primary victims but also secondary ones that they steal content from to reuse to spear-phish primary targets. One interesting incident involves compromising the email account of a famous Israeli engineer to get nonpublic documents from him. These were then used to more convincingly mimic the engineer in order to get to primary targets within his professional circle.

As previously mentioned, Rocket Kitten will keep trying to hit targets and won't rest until they do. This can mean receiving the same email five or ten times, perhaps with slightly different words, prompting receivers to click fatal links. If one method or email content does not work, the attackers will resort to different wording. Rocket Kitten, in this sense, is not only persistent but also very agile. The attackers:

- Keep finding new cover stories by making them up based on stolen information
- Use various email addresses (faked or breached)
- Use disguises (fake identities or usurped real ones), camouflaging as people others theoretically trust
- Make phone calls and send messages, sometimes even directly corresponding with victims in order to gain genuine trust
- Breach websites to set up phishing pages (Google Drive or fake Gmail pages) or register new domains solely for phishing

In a case we analyzed, for example, one of the targets sent a message back in Hebrew, asking if the email was real. The attackers responded right away, also in Hebrew, confirming the email's authenticity. This convinced the targets to open the attached files.

Fake profiles: A case

One of Rocket Kitten's targets was lured into communicating via a fake Facebook profile. The attacker behind the fake profile communicated in perfect Farsi. This fake profile was closed by Facebook because it did not conform to community standards. This prompted the attacker to just create a new account "mah.asf.xxx" where "xxx" is a random number.

While we found no evidence that these Facebook accounts were actually handled by the Rocket Kitten Group, the conversations and additional emails from a sender with the same name strongly suggest this was indeed performed by the threat actors. The target also received emails from *[REDACTED]_asf@yahoo.com*. This account's owner attempts to build trust and/or gather information. Incidentally, this new fake Facebook profile also sent an invite request to one of ClearSky's researchers, which we will go into detail later on. In our experience, this is something that very rarely happens.

One more backdoor installer was found in the wild. This also communicated with a C&C server (*84.11.146.62*) and usurped Trend Micro HouseCall.[1] We found no traces of this backdoor installer in any spear-phishing campaign but it may have been used by the attackers to infect the systems of targets that we are not aware of. We just found it noteworthy that this installer has the same functions and uses the same C&C server.

Malware used

Rocket Kitten's entire way of launching attacks suggests that the group is not very technically sophisticated.

The same is true about the malware they utilize. Closer analysis of their code showed deficits and mistakes that a professional cybercriminal would not make (the keylogger was badly developed and easily leaked their File Transfer Protocol [FTP] credentials, for example). Modifying an existing piece of commercial code like that of Core Impact Pro did not require a lot of skill as well.

Most of the malware they use may not have been developed by the group's members. The threat actors used off-the-shelf and low-quality tools that seem to have been self-developed or made by someone for their exclusive use. The malware used to infect computers often showcased many extra features like stealth (once a payload is placed in memory, any trace of the malware on the file system is erased). A more detailed analysis of the different malware types is provided in the next chapters where we look at one specific tool (a keylogger named TSPY_WOOLERG) and analyzed malicious files used in new cases.

A new version of TSPY_WOOLERG emerges

In Operation Woolen-Goldfish, Trend Micro revealed the existence of a previously unknown keylogger dubbed "TSPY_WOOLERG." This seems to have been developed by the Rocket Kitten Group or bought for exclusive use from a third party. This keylogger showed the following debug string in its first-seen version:

```
C:\Users\Wool3n.H4t\Documents\Visual Studio 2010\Projects\C-CPP\CWoolger\Release\
CWoolger.pdb
```

1 **Fake Trend Micro HouseCall installer:** *HousecallLauncher.exe (*SHA-1: *af364ff503da71875b6d7c401a1e98e31450a561)*

We discovered a new TSPY_WOOLERG version in the wild and found different variants containing the following debug strings:

```
D:\Yaser Logers\optimizer\WoolenLoger\obj\x86\Release\windows optimizer.pdb

D:\Yaser Logers\optimizer tmp\WoolenLoger\obj\x86\Release\windows optimizer.pdb

D:\Yaser Logers\CWoolger\Release\CWoolger.pdb
```

"Yaser" is a very common Arab first name. We couldn't find other malware families with similar debug strings. We suspect Yaser to be a developer who is part of the Rocket Kitten Group or from a third party whom the group may have purchased the keylogger from. Yaser could also be the same person as "Wool3n. H4t" whom we exposed in Operation Woolen-Goldfish since the previous debug strings showed that a Wool3n.H4t was also in possession of the CWoolger source code. It could, of course, also simply be fake information that attackers intentionally put there to lead us to a false track.

The new binaries we found were compiled between 31 May and 1 August 2015. The keylogger is basically the same, yet a very basic layer of encryption has been added to hide the attackers' FTP credentials.

```
private static string win32dll(string s)
{
    string text = "";
    for (int i = 0; i < s.Length; i++)
    {
        text += (s[i] ^ '%').ToString();
    }
    return text;
}
```

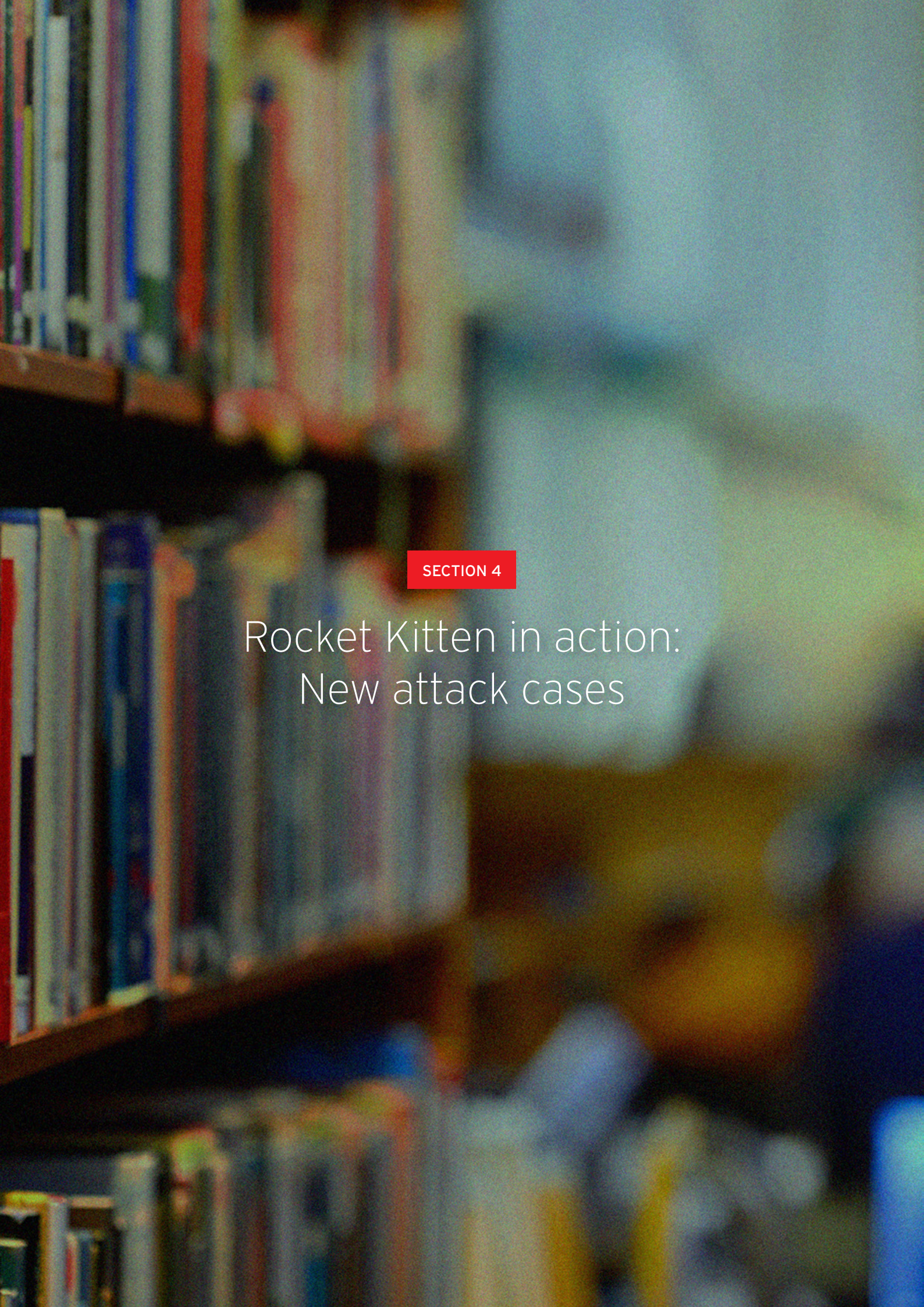
Very basic encryption used to hide the FTP credentials in the keylogger binary

The FTP server to which the stolen key logs are sent is currently set to *107.6.172.54/woolen/*. Previous versions of the keylogger also reported to the IP address, *107.6.181.116*, which belongs to the same provider, SingleHop. We noticed that some versions of the keylogger have had the upload function removed. Instead, another binary in the same folder that was externally executed was added.

Trend Micro detection	SHA-1 hash	Credential theft	Upload function	Key log file name
TSPYWOOLERG.C	db2b8f49b4e76c2f538a3a6b222c35547c802cef	No	No	%TEMP%\AdobeARM.log
	29968b0c4157f226761073333ff2e82b588ddf8e	Yes	Yes	%TEMP%\wlg.dat
	eeb67e663b2fa980c6b228fc2e04304c8992401d	Yes	Yes	%TEMP%\wlg.dat
TSPYWOOLERG.B	c8096078f0f6c3fbb6d82c5b00211802168f9cba	No	Replaced with *wsnd.exe*	%TEMP%\AdobeARMM.log

New TSPY_WOOLERG variants

The newest versions based on compilation date do not have credentials. This suggests that CWoolerg is continuously being developed, not for updating purposes or adding functionality but rather to enhance stealth so they will not be detected by security products.



SECTION 4

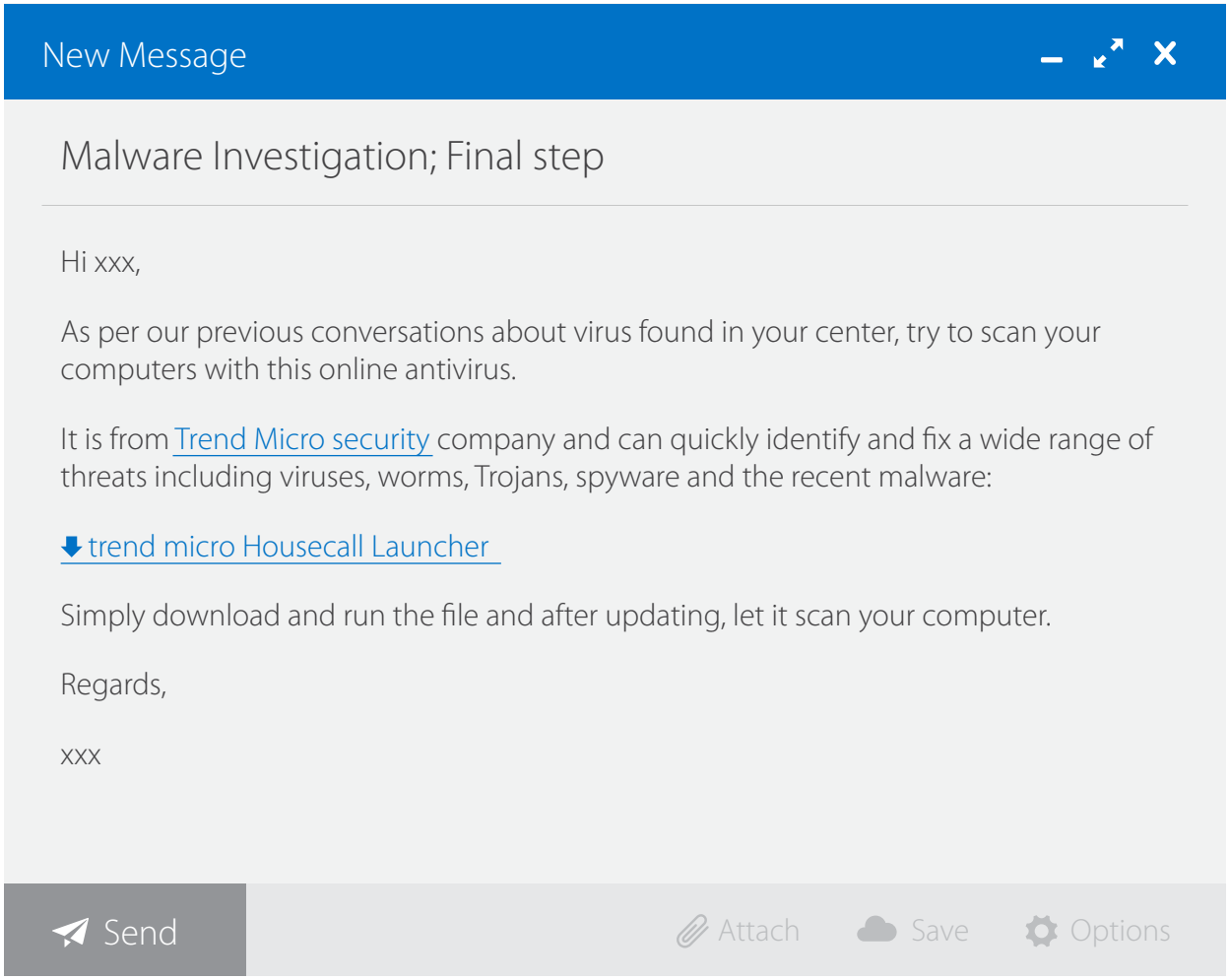
Rocket Kitten in action: New attack cases

Rocket Kitten in action: New attack cases

Case exploiting a ClearSky researcher's identity

We made an interesting observation in one particular case where the attackers attempted to approach a ClearSky threat researcher using a fake Facebook profile. When this attempt didn't work, they resorted to other techniques. In the latter part of this June, the researcher received a phone call from another attack target whom he had been in contact with during the Thamar Reservoir investigation. This other person wanted to confirm if the researcher indeed sent him an email (which he actually never did). This is just another example of the clever use of social engineering that the Rocket Kitten Group adopted to go after targets. Usurping a threat researcher's identity is something we haven't seen until now. But it tells us a back story. The attackers may either have had access to an email account revealing correspondence between the researcher and the victim or they realized that they were being investigated by ClearSky and exploited that knowledge.

The attackers used the researcher's real email signature as camouflage in order to send this legitimate-sounding content to the victim:



Spear-phishing email received by a target supposedly from a ClearSky researcher

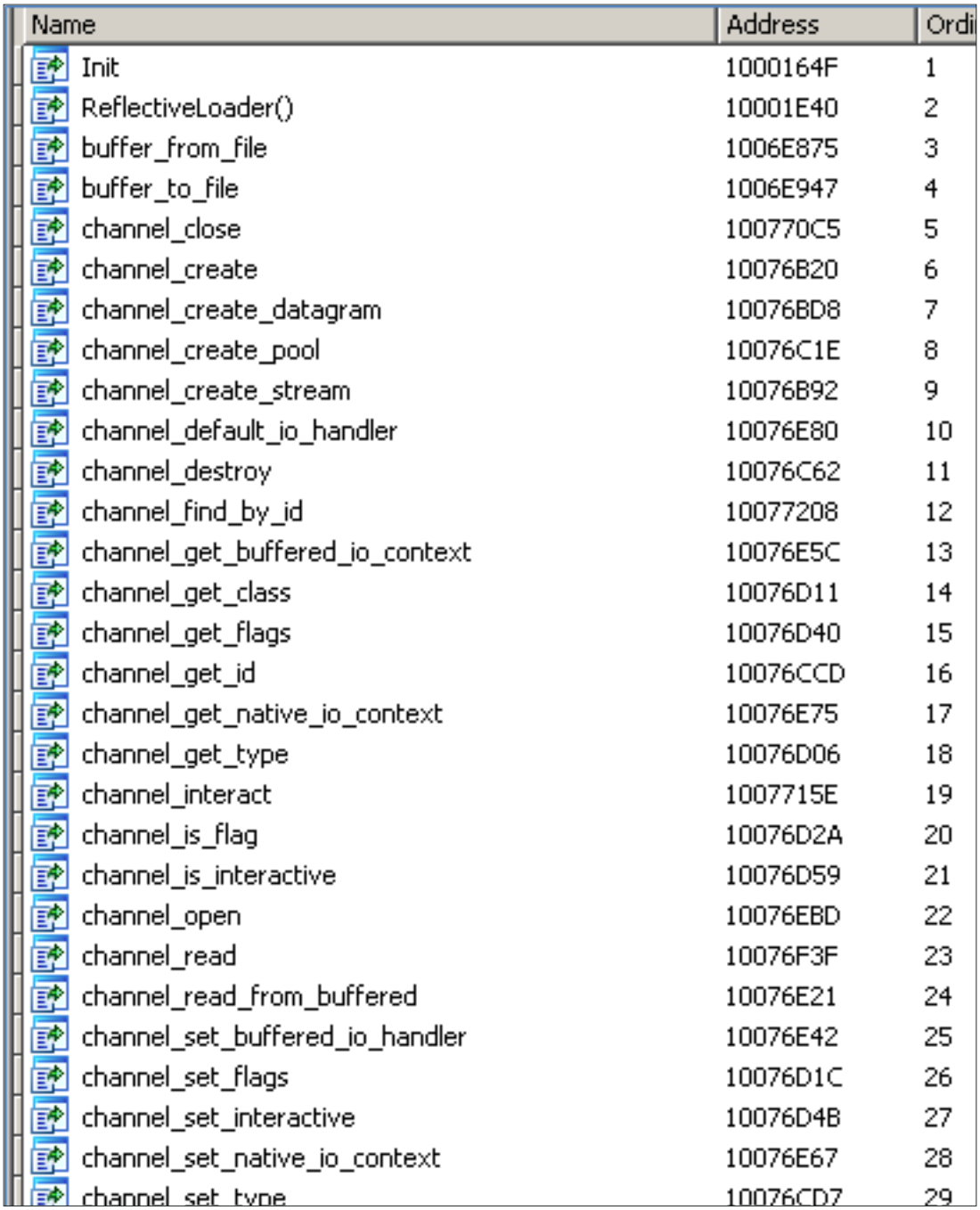
Technical analysis

In this particular case, we can't reveal the victim's name or any other specific circumstances but we did find some noteworthy technical details, including:

- The email was sent using the address, *clearsky.cybersec.group@gmail.com*, which is obviously not an official ClearSky address that the attackers created. Attentive recipients should realize that the important information here lies in the address domain—a Gmail address—but very often, they tend to intuitively only react to the first part of the name that indicates some kind of security problem with their machines.
- The first link in the email, "Trend Micro security," actually leads to the real Trend Micro website, *trendmicro.com*.

- The second link that the recipients are supposed to click in order to download HouseCall, however, leads to a malicious file *(HousecallLauncher.exe* [SHA-1: *af364ff503da71875b6d7c401a1e98e31450a561])*.
- The attackers' choice to use the Trend Micro brand as lure raised a red flag. It could have either been a purely random choice or a very cleverly chosen one. Knowing that Trend Micro investigated on their operations, they could have utilized this fact to create a false sense of security and trust with victims who would probably believe it safe to download the vendor's product. Perhaps this is also a payback for revealing details on one of their operations.
- The malicious file *(HousecallLauncher.exe)* is a Flex-compressed .SFX file with a lot of obfuscation and anti-debugging code. It has three embedded files, namely:
  - ***Data.ini:*** Only contains a path to the actual file.
  - ***FILE1:*** An official Trend Micro HouseCall launcher binary.
  - ***FILE2* (SHA-1: *457f54e9a0f32f2648f95a8e339d9fd9aed23fa7):*** The actual malicious payload—a Meterpreter[2] stager.
- When the .SFX file is executed, the payload is placed and ran in memory. No traces are left in the file system, rendering detection rather difficult.
- It accesses the same IP address *(84.11.146.62),* which belongs to IABG in Germany. This service provider has already been used in previous Rocket Kitten operations. The malware obfuscates every application programming interface (API) string in its body (using a simple XOR operation with the value, *0xC4h)*. It also very carefully obfuscates its strings after use.
- The code is literally littered with several anti-debugging techniques (IsDebuggerPresent, GetTickCount, and ZwQueryInformationProcess tricks).
- The code only has one function—to establish a connection with the IP address, *84.11.146.62,* in order to download a new binary. Once connected to the C&C server, the downloaded binary is injected into a process, which is, in fact, *metsrv.dll,* from Metasploit. It has several export functions.

2 *Meterpreter is an advanced, dynamically extensible payload included in the Metasploit framework. It can provide complex and advanced features that would otherwise be tedious to purely implement in assembly. Developers can write their own extensions in .DLL files that can be uploaded and injected into processes running on target computers after exploitation.*



Name	Address	Ordi
Init	1000164F	1
ReflectiveLoader()	10001E40	2
buffer_from_file	1006E875	3
buffer_to_file	1006E947	4
channel_close	100770C5	5
channel_create	10076B20	6
channel_create_datagram	10076BD8	7
channel_create_pool	10076C1E	8
channel_create_stream	10076B92	9
channel_default_io_handler	10076E80	10
channel_destroy	10076C62	11
channel_find_by_id	10077208	12
channel_get_buffered_io_context	10076E5C	13
channel_get_class	10076D11	14
channel_get_flags	10076D40	15
channel_get_id	10076CCD	16
channel_get_native_io_context	10076E75	17
channel_get_type	10076D06	18
channel_interact	1007715E	19
channel_is_flag	10076D2A	20
channel_is_interactive	10076D59	21
channel_open	10076EBD	22
channel_read	10076F3F	23
channel_read_from_buffered	10076E21	24
channel_set_buffered_io_handler	10076E42	25
channel_set_flags	10076D1C	26
channel_set_interactive	10076D4B	27
channel_set_native_io_context	10076E67	28
channel_set_type	10076CD7	29

List of export functions in the binary

In sum, the first binary only contains instructions to contact the handler, read the 4-byte value (the size of the *metsrv.dll* file), allocate the required RWX memory in the remote host, download the *metsrv.dll* file, and through a process known as "reflective DLL injection," pass the control to the *metsrv.dll* file.

The Thamar Gindin case: Thamar Reservoir

ClearSky's Thamar Reservoir research revealed attacks against Dr. Thamar E. Gindin, an expert on Iranian linguistics and pre-Islamic Iran, lecturer, and research fellow at the Ezri Center for Iran and Persian Gulf Research at the University of Haifa. The attack dates back to mid-2015. In an interview with the IDF radio station, she revealed connections to and communications with people in Iran.[3] It's not difficult to imagine that her pronounced opinions can make her profile disturbing in a certain context.

Before ClearSky's publication, the attackers already attempted to victimize Dr. Gindin using different techniques, including:

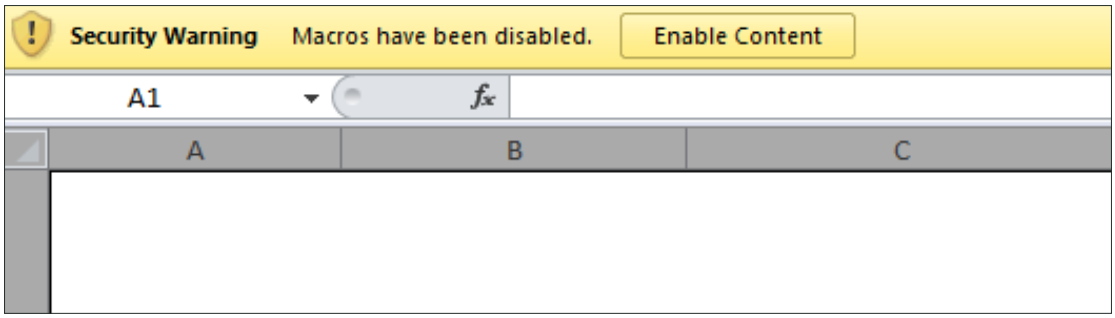
- A malware-laden spear-phishing email
- Three separate emails with links to fake log-in pages (including those that require two-factor authentication), one of which was hosted on a breached website while another two had dedicated domains
- Two phone calls from the attackers designed to build rapport for the purpose of phishing
- Numerous attempts to take over her cloud accounts using the providers' account-recovery mechanisms
- Numerous Facebook messages and emails

It's interesting to note that ClearSky's publication didn't really deter the attackers from continuing their actions. Rather, they kept on trying to hack into Dr. Gindin's email accounts even though she was already aware that she was being targeted. This June, after the release of ClearSky's research, Dr. Gindin received notifications from Google that they received password-reset requests that she never made.

The attackers can be said to have taken the following steps:

- They created a Gmail account with a username that only differed by one character from Dr. Gindin's. They used this account to send emails with an Excel spreadsheet attachment named "*Message.xlsb* (SHA-1: *46a995df8d9918ca0793404110904479b6adcb9f,* detected by Trend Micro as "X2KM_MDROP.A") to several of Dr. Gindin's contacts.
- Opening the .XLSB file asks the recipient to enable macros.

3 http://gulfc.haifa.ac.il/index.php/the-ezri-center-in-the-media/291-the-ezri-center-in-the-media



Prompt to enable macros that recipients see

- Enabling macros results in BKDR_SWRORT.CP infection. Users see some academic content in Hebrew (a timeline of events for the faculty for 2015). What struck us is that the Excel file was created the same day the email was sent. This tells us that the attackers customized the document for this spear phishing and did not simply reuse old content. Members of the group often seemed to use stolen nonpublic documents as lure. This is a favorite Rocket Kitten technique.
- The backdoor installation is fairly straightforward. A file called "*tmp.bat*" is created in the infected systems' root folder and executed.

```
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "My
App" /t REG_SZ /F /D "C:\Users\#USERNAME#\NTUSER.dat{GUID}.exe"

del tmp.bat
```

Temporary script created on an infected system

The script only has two lines of code:

- The first line adds a "run" registry key to make the file *NTUSER.dat{GUID}.exe* persistent. This is vital because it ensures that the backdoor will relaunch every time an infected computer is rebooted. Also, note that the Globally Unique Identifier (GUID)[4] is unique for each run (for example, *C83519C4-C8FE-4AB2-9061-A6B3D7525FC9)*. Randomizing the GUID is a way to bypass malware detection based on file name. Using the same file name makes a piece of malware easy to detect.

4 *GUID is a unique reference number. It's a 128-bit value that is unique not only within an enterprise but also worldwide. Active Directory internally uses GUID to identify objects.*

- The second line deletes the script in an attempt to hide the infection.
- The file, *NTUSER.dat{GUID}.exe* (SHA-1: *64ba130e627dd85c85d6534e769d239080e068dd*, detected by Trend Micro as "BKDR_SWRORT.CP") has been dropped prior to launching the *tmp.bat* script.

- BKDR_SWRORT.CP is a small downloader that communicates with and downloads files from the IP address, *84.11.146.62*. This IP address belongs to an IABG IP range (http://www.iabg.de/), a German satellite communications provider that the attackers have been using for a long time.

Conclusion

Conclusion

The Rocket Kitten Group has been around for a while now. Based on research done by several security companies, including Trend Micro and ClearSky, we can assume that their activities will continue in the near future, as they weren't deterred by making their existence and attack methods known.

We've been observing the group for about a year now. The more information we gather about their tactics and methods, the more we are convinced that what we are facing is a group of resourceful and persistent actors. Rocket Kitten doesn't need sophisticated skills. The infection vectors that the group uses are very simple. The malware they use are mostly purchased from third parties. But these shouldn't fool anyone into thinking they're less difficult to deal with. Rocket Kitten makes up for their shortcomings by being extremely persistent and agile. The cases we analyzed in this paper show that careful planning and creativity are involved when they attempt to gain access to and gain a foothold in a target.

Targeted attacks are not only used for economic advancement via stealing. Rather, they should be considered an evolution of the tradecraft of classic espionage, even in geopolitical relations.

Appendix

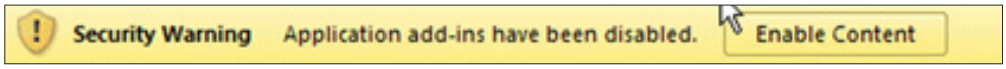
General safety measures against targeted attacks

- **Be vigilant; share information.** First, be vigilant. The second has to do with information sharing. If you think or know that you are being targeted, it helps to be familiar with and conscious of the attackers' modus operandi. Therefore, examining emails, websites, and other forms of communication can help you identify threats and avoid infection. Ask questions like "Do you know the sender?"; "Is this his address?"; and "Does it make sense for him to use or send macros?" When attack targets share information with colleagues, friends, and family members, the attackers have a harder time fooling them. And if security analyses are available to investigate suspicious emails, files, and websites, it is even more crucial to share information. This helps you understand their tools and methods, technical infrastructure, targets, and, perhaps, even their aims and objectives.
- **Seek specialists' assistance in case of an attack.** Even if you know that you are being attacked, you still need professional guidance from specialists who can analyze incidents and provide real-time assistance. This is even more significant if attacks succeed. For example, attackers may execute numerous password-reset attempts at the same time, making you believe you're losing control of your accounts. Without professional guidance, you can make a mistake like give your credentials to an attacker, click a malicious link, or even neglect to inform your service provider that account restoration should be canceled. The usual initial reaction to receiving suspicious messages is to delete them. However, reporting suspicious messages to your organization's security team is crucial so they can analyze attack methods, assess risks, and identify malicious content.
- **Regularly and timely update software.** We can never repeat this enough—OSs and installed software must be constantly updated with security fixes.
- **Use up-to-date anti-malware solutions and Host Intrusion Prevention Systems (HIPSs).** These software help detect threats.
- **Regularly run network checks.** If you run a network, regularly check log files or have them checked by a security professional. This will help you discover malicious communication with attackers and C&C servers.

Specific measures related to Rocket Kitten

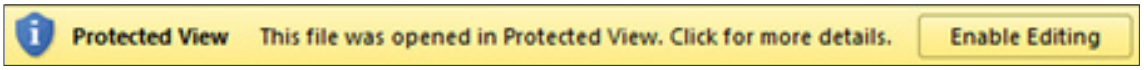
- **Pay close attention to senders' addresses even if they seem familiar.** The fact that a message is part of a previous conversation does not mean that it is authentic (it could be an indication that the attacker took control of someone else's account). We have already seen email addresses with minor changes used (one different letter in the address or domain and therefore seem identical at first sight).
- **Do not enter your password on pages you were led to by links embedded in emails.** It's always better to manually type desired domain addresses, search for them on Google, or use bookmarked links.

- **Inform acquaintances about attacks.** They can become targets as well.
- **Known and "trusted" websites can be hacked and used as part of an attack infrastructure.** Never automatically trust any website. Always closely check websites and messages and look for unreasonable mistakes (grammar, typos, etc.).
- **Immediately report suspicious incidents.** You may not have adequate professional knowledge and understanding of an attack. Therefore, it is vital to notify your organization's cybersecurity team of any suspicious incident. An example of this is receiving Facebook messages asking you to reset your password or informing you of unauthorized access to your email account from an unknown user.



- **Always flag macro-laden files as "very suspicious."** Report them to your security team except if you regularly work with macros. Asking you to "Enable Content" is very suspicious.

  While IT and security professionals immediately understand what the message means, most users don't. Nonetheless, you should become familiar with this specific message (which is almost always suspicious), as opposed to the "Protected View" message that doesn't imply if opening a file is safe or unsafe.



References

1. Cedric Pernet and Kenney Lu. (2015). *Trend Micro Security Intelligence*. "Operation Woolen-Goldfish: When Kittens Go Phishing." Last accessed on 25 August 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-woolen-goldfish.pdf.

2. ClearSky. (4 September 2014). *ClearSky Cyber Security Blog*. "Gholee—A 'Protective Edge'-Themed Spear-Phishing Campaign." Last accessed on 25 August 2015, http://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/.

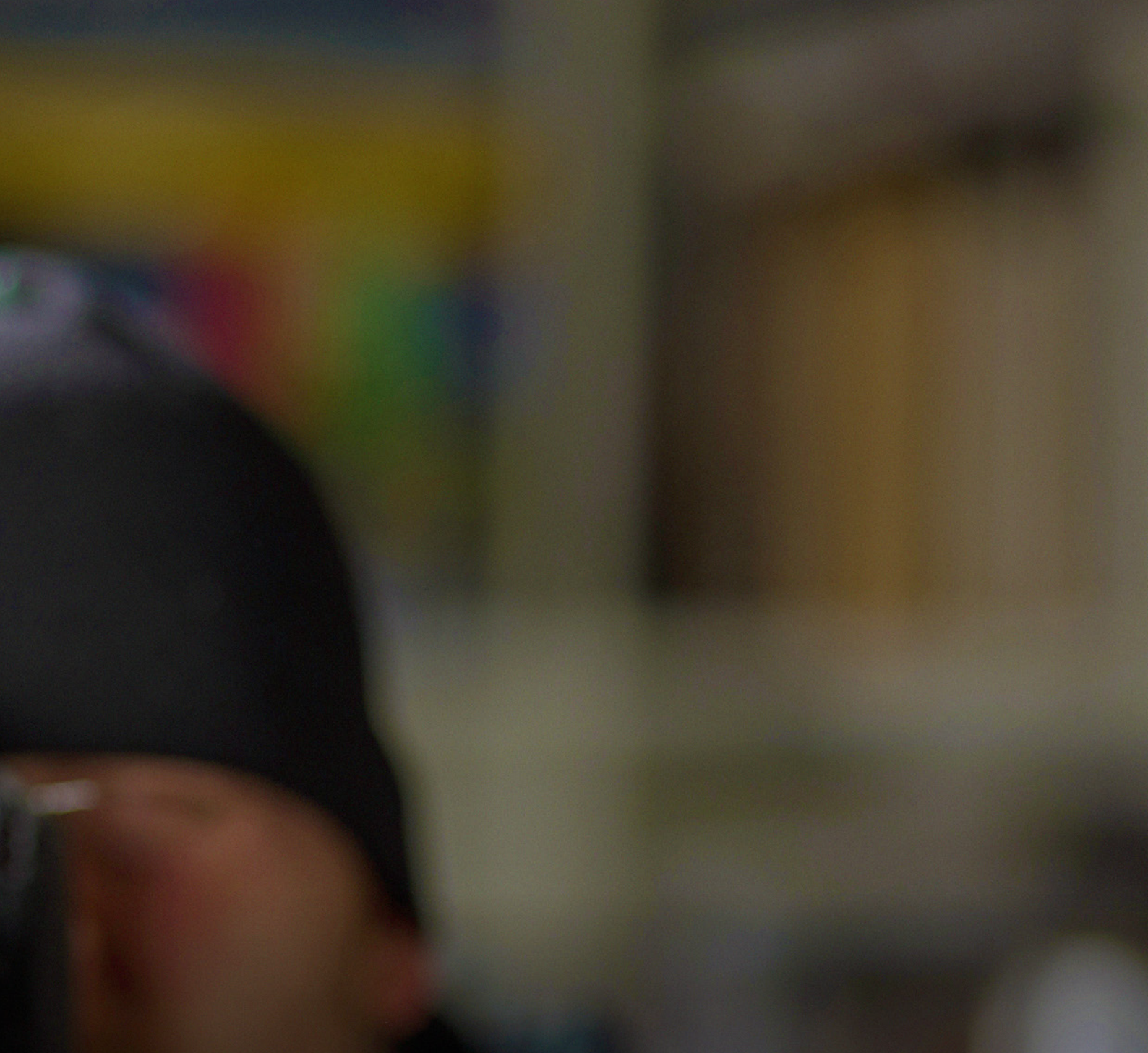
3. ClearSky. (2015). *ClearSky Cyber Security Blog*. "Thamar Reservoir: An Iranian Cyber Attack Campaign Against Targets in the Middle East." Last accessed on 27 August, 2015, http://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf.

4. CCCen. (28 December 2014). *YouTube*. "Rocket Kitten: Advanced Off-the-Shelf Targeted Attacks Against Nation-States [31c3]." Last accessed on 25 August 2015, https://www.youtube.com/watch?v=WIhKovlHDJo.

5. Cedric Pernet. (18 March 2015). *TrendLabs Security Intelligence Blog*. "Operation Woolen-Goldfish: When Kittens Go Phishing." Last accessed on 25 August 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/operation-woolen-goldfish-when-kittens-go-phishing/.

6. ClearSky. (3 June 2015). *ClearSky Cyber Security Blog*. "Thamar Reservoir—An Iranian Cyber Attack Campaign Against Targets in the Middle East." Last accessed on 25 August 2015, http://www.clearskysec.com/thamar-reservoir/.

7. Rika Joi Gregorio. (10 April 2015). *Trend Micro Threat Encyclopedia*. "TSPY_WOOLERG.A." Last accessed on 25 August 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TSPY_WOOLERG.A.



Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud