When Governments Hack Opponents: A Look at Actors and Technology

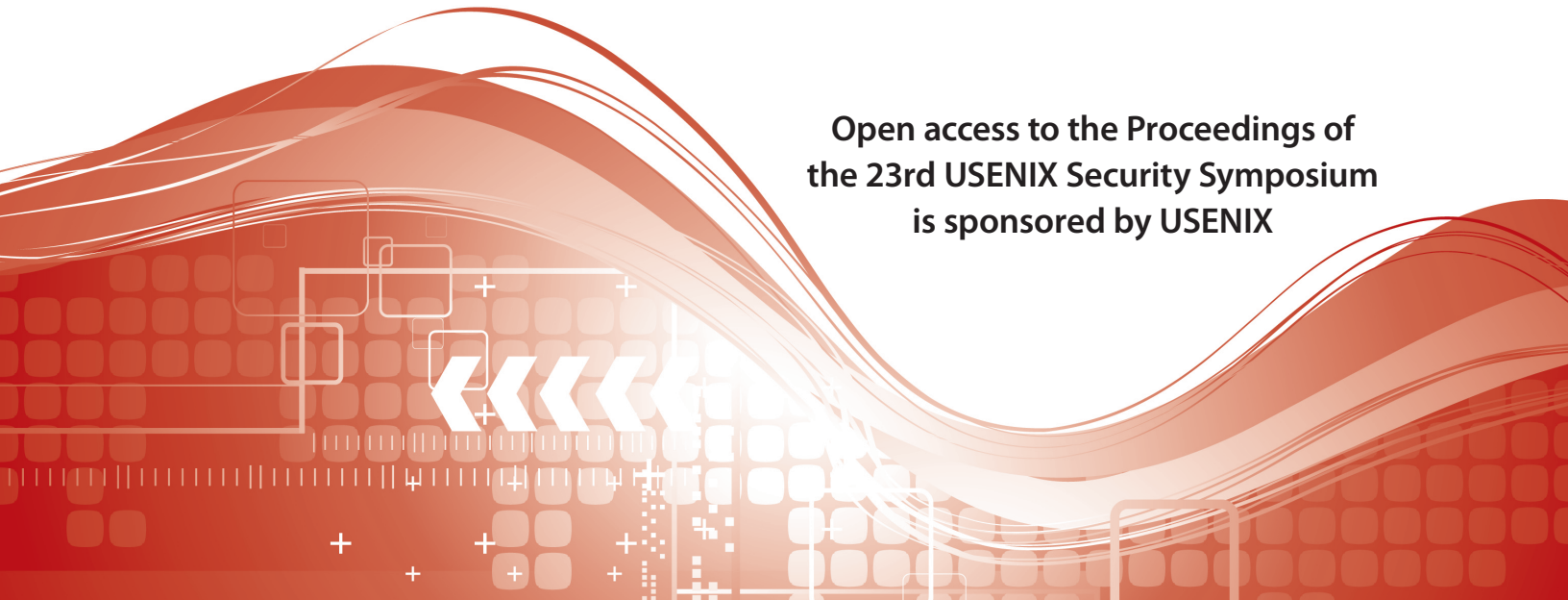
William R. Marczak, ***University of California, Berkeley, and The Citizen Lab;***
John Scott-Railton, ***University of California, Los Angeles, and The Citizen Lab;***
Morgan Marquis-Boire, The ***Citizen Lab;*** **Vern Paxson,** ***University of California, Berkeley, and International Computer Science Institute***

https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/marczak

This paper is included in the Proceedings of the 23rd USENIX Security Symposium.

August 20–22, 2014 • San Diego, CA

ISBN 978-1-931971-15-7



Open access to the Proceedings of the 23rd USENIX Security Symposium is sponsored by USENIX

When Governments Hack Opponents: A Look at Actors and Technology

William R. Marczak
UC Berkeley, Citizen Lab

John Scott-Railton
UCLA, Citizen Lab

Morgan Marquis-Boire
Citizen Lab

Vern Paxson
UC Berkeley, ICSI

Abstract

Repressive nation-states have long monitored telecommunications to keep tabs on political dissent. The Internet and online social networks, however, pose novel technical challenges to this practice, even as they open up new domains for surveillance. We analyze an extensive collection of suspicious files and links targeting activists, opposition members, and non-governmental organizations in the Middle East over the past several years. We find that these artifacts reflect efforts to attack targets' devices for the purposes of eavesdropping, stealing information, and/or unmasking anonymous users. We describe attack campaigns we have observed in Bahrain, Syria, and the United Arab Emirates, investigating attackers, tools, and techniques. In addition to off-the-shelf remote access trojans and the use of third-party IP-tracking services, we identify commercial spyware marketed exclusively to governments, including Gamma's FinSpy and Hacking Team's Remote Control System (RCS). We describe their use in Bahrain and the UAE, and map out the potential broader scope of this activity by conducting global scans of the corresponding command-and-control (C&C) servers. Finally, we frame the real-world consequences of these campaigns via strong circumstantial evidence linking hacking to arrests, interrogations, and imprisonment.

1 Introduction

Computer security research devotes extensive efforts to protecting individuals against indiscriminate, large-scale attacks such as those used by cybercriminals. Recently, the problem of protecting institutions against targeted attacks conducted by nation-states (so-called "Advanced Persistent Threats") has likewise elicited significant research interest. Where these two problem domains intersect, however—targeted cyber attacks by nation-states against *individuals*—has received virtually no significant, methodical research attention to date. This new problem space poses challenges that are both technically complex and of significant real-world importance.

In this work we undertake to characterize the emergent problem space of nation-state Internet attacks against individuals engaged in pro-democracy or opposition movements. While we lack the data to do so in a fully comprehensive fashion, we provide extensive detail from both technical and operational perspectives as seen in three countries. We view such characterizations as the fundamental first step necessary for the rigorous, scientific pursuit of a new problem space.

For our study we draw upon several years of research we have conducted into cases from Bahrain, Syria and the United Arab Emirates. We frame the nature of these attacks, and the technology and infrastructure used to conduct them, in the context of their impacts on real people. We hope in the process to inspire additional research efforts addressing the difficult problem of how to adequately protect individuals with very limited resources facing powerful adversaries.

As an illustration of this phenomenon, consider the following anecdote, pieced together from public reports and court documents.

At dawn on 3/12/13,[1] police raided the house of 17-year-old Ali Al-Shofa, confiscated his laptop and phone, and took him into custody. He was charged with referring to Bahrain's King as a "dictator" (الطاغية) and "fallen one" (الساقط) on a pseudonymous Twitter account, `@alkawarahnews`. According to court documents, Bahrain's Cyber Crime Unit had linked an IP address registered in his father's name to the account on 12/9/12. Operators of `@alkawarahnews` later forwarded a suspicious private message to one of the authors. The message was received on 12/8/12 on a Facebook account linked to the Twitter handle, and contained a link to a protest video, purportedly sent by an anti-government individual. The link redirected through `iplogger.org`, a service that records the IP address of anyone who clicks. Analytics for the link indicate that it had been clicked once from inside Bahrain. On 6/25/13, Ali was sentenced to one year in prison.

Ali's case is an example of the larger phenomenon we investigate: attacks against activists, dissidents, trade unionists, human rights campaigners, journalists, and members of NGOs (henceforth "targets") in the Middle East. The attacks we have documented usually involve the use of malicious links or e-mail attachments, designed to obtain information from a device. On the one hand, we have observed attacks using a wide range of off-the-shelf spyware, as well as publicly available third-party services, like `iplogger.org`. On the other hand, some attacks use so-called "lawful intercept" trojans and related equip-

[1] Dates in the paper are given MM/DD/YY.

ment, purportedly sold exclusively to governments by companies like Gamma International and Hacking Team. The latter advertises that governments need its technology to "look through their target's eyes" rather than rely solely on "passive monitoring" [1]. Overall, the attacks we document are rarely technically novel. In fact, we suspect that the majority of attacks could be substantially limited via well-known security practices, settings, and software updates. Yet, the attacks are noteworthy for their careful social engineering, their links to governments, and their real-world impact.

We obtained the majority of our artifacts by encouraging individuals who might be targeted by governments to provide us with suspicious files and unsolicited links, especially from unfamiliar senders. While this process has provided a rich set of artifacts to analyze, it does not permit us to claim our dataset is representative.

Our analysis links these attacks with a common class of actor: an attacker whose behavior, choice of target, or use of information obtained in the attack, aligns with the interests of a government. In some cases, such as Ali's, the attackers appear to be governments themselves; in other cases, they appear instead to be pro-government actors, ranging from patriotic, not necessarily skilled volunteers to cyber mercenaries. The phenomenon has been identified before, such as in Libya, when the fall of Gaddafi's regime revealed direct government ties to hacking during the 2011 Civil War [2].

We make the following contributions:

- We analyze the technology associated with targeted attacks (e.g., malicious links, spyware), and trace it back to its programmers and manufacturers. While the attacks are not novel—and indeed often involve technology used by the cybercrime underground—they are significant because they have a real-world impact and visibility, and are connected to governments. In addition, we often find amateurish mistakes in either the attacker's technology or operations, indicating that energy spent countering these threats can realize significant benefits. We do not, however, conclude that all nation-state attacks or attackers are incompetent, and we suspect that some attacks have evaded our detection.
- When possible, we empirically characterize the attacks and technology we have observed. We map out global use of two commercial hacking tools by governments by searching through Internet scan data using fingerprints for command-and-control (C&C) servers derived from our spyware analysis.
- We develop strong evidence tying attacks to government sponsors and corporate suppliers, countering denials, sometimes energetic and sometimes indirect, of such involvement [3, 4, 5, 6], in contrast to denials [7] or claims of a corporate "oversight" board [8]. Our scanning suggests use of "lawful intercept" trojans by 11 additional countries considered governed by "authoritarian regimes." We believe that activists and journalists in such countries may experience harassment or consequences to life or liberty from government surveillance.

Finally, we do not explore potential defenses appropriate for protecting the target population in this work. We believe that to do so in a sufficiently well-grounded, meaningful manner first requires developing an understanding of the targets' knowledge of security issues, their posture regarding how they currently protect themselves, and the resources (including potentially education) that they can draw upon. To this end, we are now conducting (with IRB approval) in-depth interviews with potential targets along with systematic examination of their Internet devices in order to develop such an understanding.

2 Related Work

In the past decades, a rich body of academic work has grown to document and understand government Internet censorship, including nationwide censorship campaigns like the Great Firewall of China [9, 10, 11]. Research on governmental Internet surveillance and activities like law-enforcement interception is a comparatively smaller area [12]. Some academic work looks at government use of devices to enable censorship, such as keyword blacklists for Chinese chat clients [13], or the Green Dam censorware that was to be deployed on all new computers sold in China [14]. We are aware of only limited previous work looking at advanced threat actors targeting activists with hacking, though this work has not always been able to establish evidence of government connections [15].

Platforms used by potential targets, such as GMail [16], Twitter [17], and Facebook [18] increasingly make transport-layer encryption the default, obscuring communications from most network surveillance. This use of encryption, along with the global nature of many social movements, and the role of diaspora groups, likely makes hacking increasingly attractive, especially to states who are unable to request or compel content from these platforms. Indeed, the increasing use of encryption and the global nature of targets have both been cited by purveyors of "lawful intercept" trojans in their marketing materials [1, 19]. In one notable case in 2009, UAE telecom firm Etisalat distributed a system update to its then 145,000 BlackBerry subscribers that contained spyware to read encrypted BlackBerry e-mail from the device. The spyware was discovered when the update drastically slowed users' phones [20]. In contrast to country-scale distribution, our work looks at this kind of pro-government and government-linked surveillance through highly *targeted* attacks.

The term APT (Advanced Persistent Threat) refers to a sophisticated cyber-attacker who persistently attempts to target an individual or group [21]. Work outside the academic community tracking government cyberattacks typically falls under this umbrella. There has been significant work on APT outside the academic community, especially among security professionals, threat intelligence companies, and human rights groups. Much of this work has focused on suspected government-on-government or government-on-corporation cyber attacks [22, 23]. Meanwhile, a small but growing body of this research deals with attacks carried out by governments against opposition and activist groups operating within, as well as outside their borders. One of the most notable cases is GhostNet, a large-scale cyber espionage campaign against the Tibetan independence movement [24, 25]. Other work avoids drawing conclusions about the attackers [26].

Country	Date Range	Range of Targets	Number and Type of Samples	Distinct Malware C&C's
Bahrain	4/9/12—7/31/13	$\geq$ 12 activists, dissidents, trade unionists, human rights campaigners, and journalists	8 FinSpy samples, 7 IP spy links received via private message, $>$ 200 IP spy links observed publicly	4 distinct IP addresses
Syria	2011 to present	10–20 individuals with technical backgrounds who receive suspect files from their contacts	40–50: predominantly BlackShades, DarkComet, Xtreme RAT, njRAT, ShadowTech RAT.	160 distinct IP addresses
UAE	7/23/12—7/31/13	7 activists, human rights campaigners, and journalists	31 distinct malware samples spanning 7 types; 5 distinct exploits	12 distinct IP addresses

Table 1: Range of data for the study.

Country	Possible Impacts	Probable Impacts
Bahrain	1. 3 individuals arrested, sentenced to 1–12 mo in prison 2. Union leader questioned by police; fired	1. Activist serving 1 yr in prison 2. Police raid on house
Syria	1. Sensitive opposition communications exposed to government 2. Exfiltrated material used to identify and detain activists	1. Opposition members discredited by publishing embarrassing materials 2. Exfiltrated materials used during interrogation by security services
UAE	Contacts targeted via malware	Password stolen, e-mail downloaded

Table 2: Negative outcomes plausibly or quite likely arising from attacks analyzed.

3 Data Overview and Implications

Our study is based on extensive analysis of malicious files and suspect communications relevant to the activities of targeted groups in Bahrain, Syria, and the UAE, as documented in Table 1. A number of the attacks had significant real-world implications, per Table 2. In many cases, we keep our descriptions somewhat imprecise to avoid potential leakage of target identities.

We began our work when contacted by individuals concerned that a government might have targeted them for cyber-attacks. As we became more acquainted with the targeted communities, in some cases we contacted targeted groups directly; in others, we reached out to individuals with connections to targeted groups, who allowed us to examine their communications with the groups. For Bahrain and Syria, the work encompassed 10,000s of e-mails and instant messages. For the UAE, the volume is several thousand communications.

4 Case Studies: Three Countries

This following sections outline recent targeted hacking campaigns in Bahrain, Syria and the UAE. These cases have a common theme: attacks against targets' computers and devices with malicious files and links. In some cases the attackers employed expensive and "government exclusive" malware, while in other cases, attackers used cheap and readily available RATs. Across these cases we find that clever social engineering often plays a central role, which is strong evidence of a well-informed adversary. We also, however, frequently find technical and operational errors by the attackers that enable us to link attacks to governments. In general, the attacks we find are not well-detected by anti-virus programs.

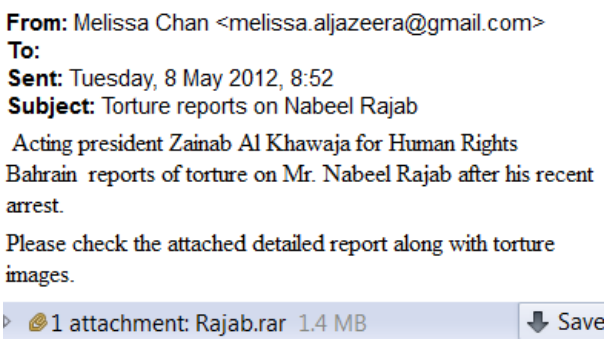


Figure 1: E-mail containing FinSpy.

4.1 Bahrain

We have analyzed two attack campaigns in the context of Bahrain, where the government has been pursuing a crackdown against an Arab-Spring inspired uprising since 2/14/2011.

The first involved malicious e-mails containing *FinSpy*, a "lawful intercept" trojan sold exclusively to governments. The second involved specially crafted *IP spy* links and e-mails designed to reveal the IP addresses of operators of pseudonymous accounts. Some individuals who apparently clicked on these links were later arrested, including Ali (cf. §1), whose click appears to have been used against him in court. While both campaigns point back to the government, we have not as yet identified overlap between the campaigns; targets of FinSpy appeared to reside mainly outside Bahrain, whereas the IP spy links targeted those mainly inside the country. We examine each campaign in turn.

FinSpy Campaign. Beginning in April 2012, the authors received 5 suspicious e-mails from US and UK-based activists and journalists working on Bahrain. We found that some of the attachments contained a PE (`.exe`) file designed to appear as an image. Their filenames contained a Unicode *right-to-left override* (RLO) character, causing Windows to render a filename such as `gpj.1bajaR.exe` instead as `exe.Rajab1.jpg`.

The other `.rar` files contained a Word document with an embedded ASCII-encoded PE file containing a custom macro set to automatically run upon document startup. Under default security settings, Office disables all unsigned macros, so that a user who opens the document will only see an informational message that the macro has been disabled. Thus, this attack was apparently designed with the belief or hope that targets would have reduced security settings.

Identification as FinSpy: By running the sample using Windows Virtual PC, we found the following string in memory: `y:\lsvn_branches\finspyv4.01\finspyv2\`. This string suggests FinSpy, a product of Gamma International [27]. The executables used virtualized obfuscation [28], which appeared to be custom-designed. We devised a fingerprint for the obfuscater and located a structurally similar executable by searching a large malware database. This executable contained a similar string, except it identified itself as `FinSpy v3.00`, and attempted to connect to `tiger.gamma-international.de`, a domain registered to Gamma International GmbH.

Analysis of capabilities: We found that the spyware has a modular design, and can download additional modules from a command & control (C&C) server, including password capture (from over 20 applications) and recording of screenshots, Skype chat, file transfers, and input from the computer's microphone and webcam.

To exfiltrate data back to the C&C server, a module encrypts and writes it to disk in a special folder. The spyware periodically probes this folder for files that match a certain naming convention, then sends them to the C&C server. It then overwrites the files, renames them several times, and deletes them, in an apparent effort to frustrate forensic analysis.

Analysis of encryption: Because the malware employed myriad known anti-debugging and anti-analysis techniques, it thwarted our attempts to attach debuggers. Since it did not include anti-VM code, we ran it in TEMU, an x86 emulator designed for malware analysis [29]. TEMU captures instruction-level execution traces and provides support for taint-tracking.

We found that FinSpy encrypts data using a custom implementation of AES-256-CBC. The 32 byte AES key and 16 byte IV are generated by repeatedly reading the low-order-4-bytes of the Windows clock. The key and IV are encrypted using an embedded RSA-2048 public key, and stored in the same file as the data. The private key presumably resides on the C&C server. The weak AES keys make decryption of the data straightforward. We wrote a program that generally can find these keys in under an hour, exploiting the fact that many of the system clock readings occur within the same clock-update quantum.

In addition, FinSpy's AES code fails to encrypt the last block of data if less than the AES block size of 128 bits, leaving trailing plaintext. Finally, FinSpy's wire protocol for C&C communication uses the same type of encryption, and thus is subject to the same brute force attack on AES keys. While we suspect FinSpy's cryptographic deficiencies reflect bugs, it is also conceivable that the cryptography was deliberately weakened to facilitate one government monitoring the surveillance of others.

C&C server: The samples communicated with `77.69.140.194`, which belongs to a subscriber of Batelco, Bahrain's main ISP. Analyzing network traffic between our infected VM and the C&C server revealed that the server used a global IPID, which allowed us to infer server activity by its progression.

In response to our preliminary work an executive at Gamma told the press that Bahrain's FinSpy server was merely a proxy and the real server could have been anywhere, as part of a claim that the Bahrain FinSpy deployment could have been associated with another government [4]. However, a proxy would show gaps in a global IPID as it forwarded traffic; our frequent observation of strictly consecutive IPIDs thus contradicts this statement.

Exploitation of captured data: Since we suspected the spyware operator would likely seek to exploit captured credentials, particularly those associated with Bahraini activist organizations, we worked with *Bahrain Watch*, an activist organization inside Bahrain. Bahrain Watch established a fake login page on their website and provided us with a username and password. From a clean VM, we logged in using these credentials, saving the password in Mozilla Firefox. We then infected the VM with FinSpy and allowed it to connect to the Bahrain C&C server. Bahrain Watch's website logs revealed a subsequent hit from `89.148.0.41`—made however to the site's homepage, rather than its login page—coming shortly after we had infected the VM. Decrypting packet captures of the spyware's activity, we found that our VM sent the password to the server exactly one minute earlier:

```
INDEX,URL,USERNAME,PASSWORD,USERNAME FIELD,
PASSWORD FIELD,FILE,HTTP 1,
http://bahrainwatch.org,bhwatch1,watchba7rain,
username,password,signons.sqlite,,
Very Strong,3.5/4.x
```

The URL provided to the server did not include the path to the login page, which was inaccessible from the homepage. This omission reflects the fact that the Firefox password database stores only domain names, not full login page URLs, for each password. Repeating the experiment again yielded a hit from the same IP address within a minute. We inspected Bahrain Watch's logs, which showed no subsequent (or previous) activity from that address, nor any instances of the same User Agent string.

IP spy Campaign. In an *IP spy* attack, the attacker aims to discover the IP address of a victim who is typically the operator of a pseudonymous social media or e-mail account. The attacker sends the pseudonymous account a link to a webpage or an e-mail containing an embedded remote image, using one of many freely-available services.[2] When the victim clicks on the link or opens the e-mail, their IP address is revealed to the attacker.[3] The attacker then discovers the victim's identity from their ISP. In one case we identified legal documents that provided a circumstantial link between such a spy link and a subsequent arrest.

Figure 2 illustrates the larger ecosystem of these attacks. The attackers appear to represent a single entity, as the activity all connects back to accounts that sent links shortened using a particular user account *al9mood*[4] on the `bit.ly` URL shortening service.

Recall Ali Faisal Al-Shufa (discussed in Section 1), who was accused of sending insulting tweets from an account

[2] e.g., `iplogger.org`, `ip-spy.com`, `ReadNotify.com`.

[3] Several webmail providers and e-mail clients take limited steps to automatically block loading this content, but e-mails spoofed to come from a trusted sender sometimes bypass these defenses.

[4] A Romanization of the Arabic word for "steadfastness."

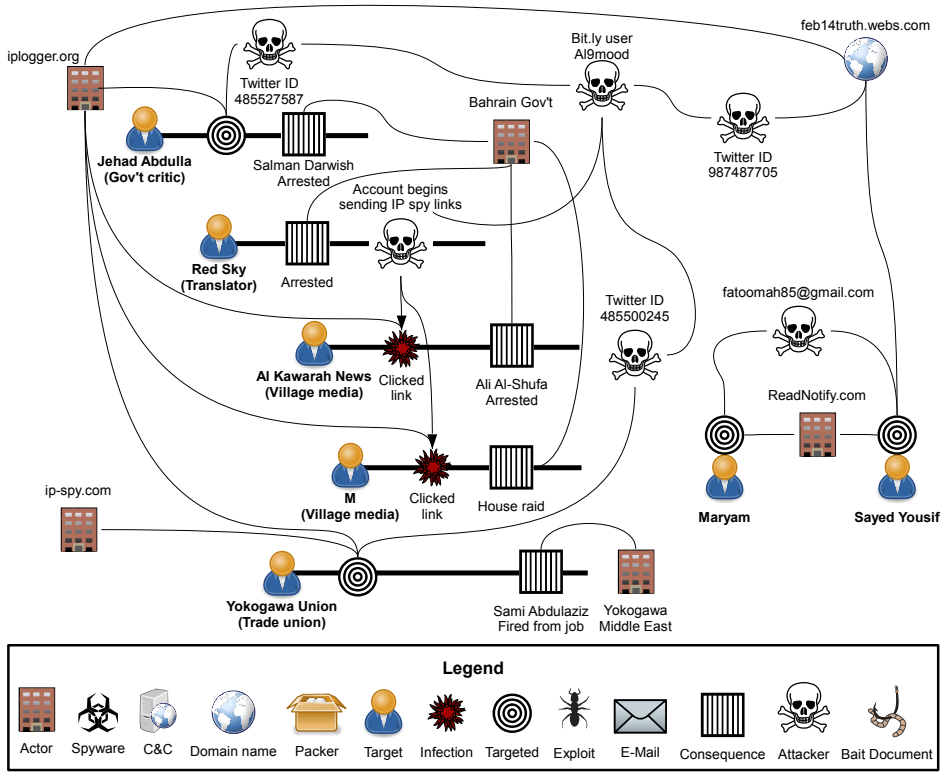


Figure 2: The ecosystem of Bahrain "IP spy" attacks.

`@alkawarahnews` (**Al Kawarah News** in Figure 2). An operator of the account forwarded us a suspicious private message sent to the Al Kawarah News Facebook account from **Red Sky**. Red Sky was purportedly arrested on 10/17/12, was convicted of insulting the King on his Twitter account `@RedSky446`, and was sentenced to four months prison.[5] When released, he found that the passwords for his Twitter, Facebook, and e-mail accounts had been changed, and did not know how to recover his accounts.

The message that Red Sky's account sent to Al Kawarah News included a link shortened using Google's `goo.gl` service. We used the `goo.gl` API to access analytics for the link, finding that it unshortened to `iplogger.org/25SX` and was created on 12/8/12. The link had received only one click, which came from Bahrain with the referrer `www.facebook.com`.

Ali's case files contained a request from the Public Prosecution for information on an IP address that it had linked to Al Kawarah News about 22 hours after the link was created. Court documents indicate that ISP data linked the IP address to Ali, and on this basis he was sentenced to one year in prison.

Red Sky also targeted **M** in Figure 2. M recalled clicking on a link from Red Sky while using an Internet connection from one of the houses in M's village. The house was raided by police on 3/12/13, who were looking for the subscriber of the house's internet connection. Police questioning revolved around Tweets that referred to Bahrain's King as a "cursed one." Red Sky had earlier targeted other users with IP spy links shortened using the *al9mood* `bit.ly` account.

The attack on **Jehad Abdulla** is noteworthy, as the account's activity aligned with communities typically critical of Bahrain's opposition. However, the account also directly criticized the King on occasion, in one case referring to him as "weak" and "stingy." An account linked to *al9mood* sent Jehad Abdulla an IP spy link on 10/2/12 in a public message. On 10/16/12, Salman Darwish was arrested for insulting the King using the Jehad Abdulla account. He was sentenced to one month in prison, partly on the basis of his confession. Salman's father claims that police denied Salman food, drink, and medical care.

Another account linked to *al9mood* targeted `@YLUBH`, the Twitter account of **Yokogawa Union**, a trade union at the Bahraini branch of a Japanese company. `@YLUBH` received at least three IP spy links in late 2012, sent via public Twitter messages. Yokogawa fired the leader of the trade union, Sami Abdulaziz Hassan, on 3/23/13 [30]. It later emerged that Sami was indeed the operator of the `@YLUBH` account, and that the police had called him in for questioning in relation to its tweets [31].

Use of embedded remote images: We identified several targets who received spoofed e-mails containing embedded remote images. Figure 2 shows two such cases, **Maryam** and **Sayed Yousif**. The attacker sent the e-mails using `ReadNotify.com`, which records the user's IP address upon

[5] According to information we received from two Twitter users, one of whom claimed to have met Red Sky in prison; another to be a colleague.

their mail client downloading the remote image.[6]

While ReadNotify.com forbids spoofing in their TOS, the service has a vulnerability known to the attackers (and which we confirmed) that allows spoofing the From address by directly setting the parameters on a submission form on their website We have not found evidence suggesting this vulnerability is publicly known, but it appears clear that the attacker exploited it, as the web form adds a X-Mailer: RNwebmail header not added when sending through ReadNotify.com's other supported methods. The header appeared in each e-mail the targets forwarded to us.

When spoofing using this method, the original sender address still appears in X-Sender and other headers. According to these, the e-mails received by the targets all came from fatoomah85@gmail.com. A link sent in one of these e-mails was connected to the *al9mood* bit.ly account.

In monitoring accounts connected to *al9mood*, we counted more than 200 IP spy links in Twitter messages and public Facebook posts. Attackers often used (1) accounts of prominent or trusted but jailed individuals like "Red Sky," (2) fake personas (e.g., attractive women or fake job seekers when targeting a labor union), or (3) impersonations of legitimate accounts. In one particularly clever tactic, attackers exploited Twitter's default font, for example substituting a lowercase "l" with an uppercase "I" or switching vowels (e.g. from "a" to an "e") to create at-a-glance identical usernames. In addition, malicious accounts tended to quickly delete IP spy tweets sent via (public) mentions, and frequently change profile names.

4.2 Syria

The use of RATs against the opposition has been a well-documented feature of the Syrian Civil War since the first reports were published in early 2012 [36, 39, 40, 32, 34]. The phenomenon is widespread, and in our experience, most members of the opposition know that some hacking is taking place. As summarized in Table 3, the attacks often include fake or maliciously packaged security tools; intriguing, or ideological, or movement-relevant content (e.g. lists of wanted persons). The seeding techniques and bait files suggest a good understanding of the opposition's needs, fears and behavior, coupled with basic familiarity with off-the-shelf RATs. In some cases attacks occur in a context that points to a more direct connection to one of the belligerents: the Syrian opposition has regularly observed that detainees' accounts begin seeding malware shortly after their arrest by government forces [41].

Researchers and security professionals have already profiled many of these RATs, including DarkComet [42, 43], Blackshades Remote Controller [38], Xtreme RAT [44], njRAT [26], and ShadowTech [36]. Some are available for purchase by anyone, in contrast to "government only" FinSpy and RCS. For example, Xtreme RAT retails for €350, while a version of Blackshades lists for €40. Others, like DarkComet, are free. We have also observed cracked versions of these RATs on Arabic-language hacker forums, making them available with little effort and no payment trail. While the RATs are cheaper and less sophisticated than FinSpy and RCS, they share the same basic functionality, including screen capture, keylogging, remote monitoring of webcams and microphones, remote shell, and file exfiltration.

In the most common attack sequence we observed, illustrated with three examples in Figure 3, the attacker seeds malware via private chat messages, posts in opposition-controlled social media groups, or e-mail. These techniques often limit the world-visibility of malicious files and links, slowing their detection by common AV products. Typically, targets receive either (1) a PE in a .zip or .rar, (2) a file download link, or (3) a link that will trigger a drive-by download. The messages usually include text, often in Arabic, that attempts to persuade the target to execute the file or click the link.

The first attacks in Figure 3 date to 2012, and use bait files with a DarkComet RAT payload. These attacks share the same C&C, 216.6.0.28, a Syrian IP address belonging to the Syrian Telecommunications Establishment, and publicly reported as a C&C of Syrian malware since February 2012 [45]. The first bait file presents to the victim as a PDF containing information about a planned uprising in Aleppo. In fact the file is a Windows Screensaver (.scr) that masquerades as a PDF using Unicode RLO, rendering a name such as ".fdp.scr" display to the victim as ".rcs.pdf." The second bait file is a dummy program containing DarkComet while masquerading as a Skype call encryption program, playing to opposition paranoia about government backdoors in common software. The third attack in Figure 3, observed in October 2013, entices targets with e-mails purporting to contain or link to videos about the current conflict, infecting victims with Xtreme RAT, and using the C&C **tn1.linkpc.net**.

For seeding, the attackers typically use compromised accounts (including those of arrested individuals) or fake identities masquerading as pro-opposition. Our illustration shows in abstract terms the use of **Victim A**'s account to seed malware ("Aleppo Plan") via (say) Skype messages to **Victim(s) B**^{n}. In the cases of **Opp. Member C** and **NGO Worker D** (here, actual victims, not abstract), targeting was by e-mail from domains apparently belonging to opposition groups, indicating a potential compromise. One domain remains active, hosting a website of the Salafist Al-Nusra front [46], while the other appears dormant. **Opp. Member C** received a malicious file as an e-mail attachment, while **NGO Worker D** was sent a shortened link (**url[.]no**/Uu5) to a download from a directory of **Mrconstrucciones[.]net**,[7] a site that may have been compromised. Both attacks resulted in an Xtreme RAT infection.

Interestingly, in the case of the fake Skype encryption the deception extended to a YouTube video from "IT Security Lab" [47] demonstrating the program's purported capabilities, as well as a website promoting the tool, **skype-encryption.sytes.net**. The attackers also constructed a basic, faux GUI for their "Encryption" program (see Figure 4). The fake GUI has a number of non-functional buttons like "Encrypt" and "DeCrypt," which generate fake prompts. While distracted by this meaningless interaction, the victim's machine is infected with DarkComet 3.3 [32, 33].

Anecdotally, campaign volume appears to track significant

[6] YahooMail and the iPhone mail client automatically load these remote images, especially in e-mails spoofed from trusted senders.

[7] Obfuscated to avoid accidental clicks on active malware URLs.

Type	Features	Examples (RATs)
Security tools	Executable files presented as a "tool" often accompanied by justifications or statements of its value in the targeted seeding, for example on a social media site, at the download location, or in videos	"Skype Encryption" (DC) [32, 33], "Facebook Security" (custom) [34], Anti-hacker (DC) [35], Fake Freegate VPN (ST) [36]
Ideologically or movement-relevant files	A document or PE as download or attachment with accompanying encouragement to open or act on the material, often masquerading as legitimate PDF documents or inadvertently leaked regime programs. Frequent use of RLO to disguise true extension (such as `.exe` or `.scr`)	"Names of individuals wanted by the Regime," (DC) "Aleppo [uprising] Plan" (DC) [37], important video (BS) [38], "Hama Rebels Council" document (DC) [39], "wanted persons" database frontend (custom), movement relevant video (njRAT), file about the Free Syrian Army (Xtreme RAT)
Miscellaneous tools	Tools pretending to offer functionality relevant to the opposition, such as a fake tool claiming to "mass report" regime pages on Facebook	hack_facebook_pro_v6.9 (DC) [40]

Table 3: Campaigns and RATs employed in Syrian surveillance. BS = Blackshades, DC = DarkComet, ST = ShadowTech.

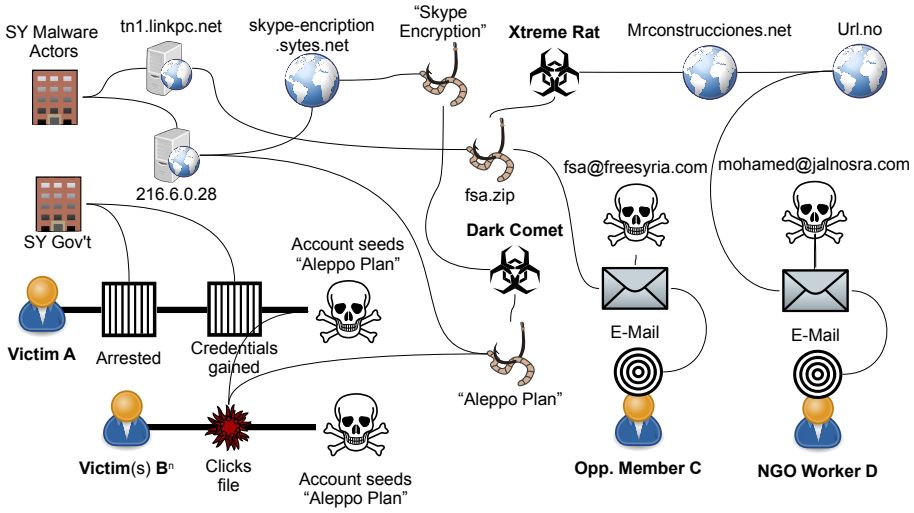


Figure 3: A sample from the ecosystem of Syrian malware campaigns.

events in the ongoing conflict. For example, campaigns dwindled and then rebounded within hours after Syria's 2012 Internet shutdown [48]. Similarly, activity observed by the authors also dwindled prior to expectation of US-led military action against Syrian government targets in September 2013. Once this option appeared to be off the table, the volume of new samples and campaigns we observed again increased, including the recent targeting of NGO workers per Figure 3. We are aware of only a negligible number of cases of the opposition using similar RATs against Syrian Government supporters, although evidence exists of other kinds of electronic attacks by third parties.

Real world consequences. The logistics and activities of Syria's numerous opposition groups are intentionally concealed from public view to protect both their efficacy, and the lives of people participating in them. Nevertheless, Syrian opposition members are generally familiar with stories off digital compromises of high-profile figures, including those entrusted with the most sensitive roles, as well as rank-and-file members. Compromise of operational security poses a documented threat to life both for victims of electronic compromise, and to family members and associates.

The Syrian conflict is ongoing, making it difficult to assem-

Figure 4: The fake Skype program distracts the victim with the promise of encrypted communications while infecting their machine with DarkComet.

ble comprehensive evidence of linkages between government actors and malware campaigns. Moreover, many individuals whose identities have been compromised are in prison or otherwise disappeared, and thus unable to relate the evidence presented to them during interrogation. Still, strong circumstantial evidence links the use of RATs, phishing, and government activity, which we briefly summarize here: (1) many Syrians have recounted to journalists and the authors how interrogators confronted them with material from their computers. For example:

> The policeman told me, "Do you remember when you were talking to your friend and you told him you had something wrong [sic] and paid a lot of money? At that time we were taking information from your laptop." [41]

(2) Syrian activists have supplied cases to international journalists [41], where arrests are quickly followed by the social media accounts of detained individuals seeding malware to contact lists (Figure 3). (3) Finally, despite the notoriety of the attack campaigns, including mention of C&C IPs in international media [45], the Syrian government has made no public statements about these campaigns nor acted to shut down the servers.

Beyond the ongoing challenges of attribution, these malware campaigns have a tangible impact on the Syrian opposition, and generally align with the interests of the Syrian government's propaganda operations. The case of Abdul Razzaq Tlass, a leader in the Free Syrian Army, is illustrative of the potential uses of such campaigns. In 2012 a string of videos emerged showing Tlass sexting and engaged in lewd activity in front of a webcam [49]. While he denied the videos, the harm to his reputation was substantial and he was eventually replaced [50].

4.3 UAE

While the UAE has experienced no recent uprising or political unrest, it has nevertheless cracked down on its opposition, concurrent with the Arab Spring.

The first attacks we observed in the UAE involved a government-grade "lawful interception" trojan known as *Remote Control System* (RCS), sold by the Italian company Hacking Team. The associated C&C server indicated direct UAE government involvement. Over time, we stopped receiving RCS samples from UAE targets, and instead observed a shift to the use of off-the-shelf RATs, and possible involvement of cyber-mercenary groups. However, poor attacker operational security allowed us to link most observed attacks together.

RCS. UAE activist **Ahmed** Mansoor (per Figure 5), imprisoned from April to November 2011 after signing an online pro-democracy petition [51], received an e-mail purportedly from "Arabic Wikileaks" in July 2012. He opened the associated attachment, "veryimportant.doc," and saw what he described as "scrambled letters". He forwarded us the e-mail for investigation.

The attachment exploited CVE-2010-3333, an RTF parsing vulnerability in Microsoft Office. The document did not contain any bait content, and part of the malformed RTF that triggered the exploit was displayed in the document. The exploit loaded shellcode that downloaded a second stage

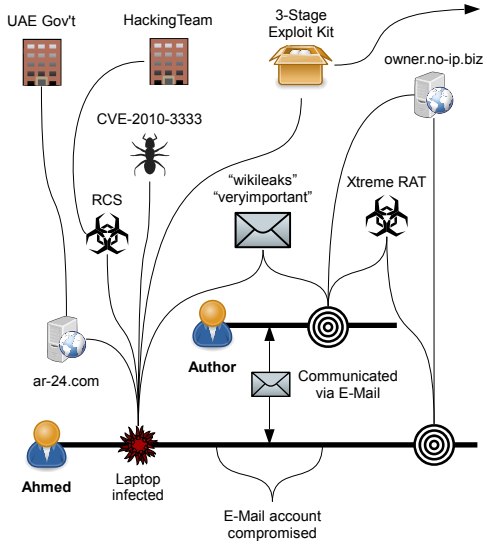


Figure 5: Part of the ecosystem of UAE surveillance attacks.

from `ar-24.com`, which in turn downloaded spyware from `ar-24.com`. We denote this combination as the **3-Stage Exploit Kit** in Figure 5.

The C&C server also ran on `ar-24.com`. When we obtained the sample in July 2012, `ar-24.com` resolved to an IP address on Linode, a hosting provider. Three months later, it resolved to a UAE address belonging to the Royal Group [52], an organization linked to the UAE government; it is chaired by Sheikh Tahnoon bin Zayed Al-Nayhan, a member of the UAE ruling family and a son of the founder of the UAE.

Identification as RCS: We identified strings in memory that matched those in a Symantec analysis [53] of RCS (also known as *DaVinci* or *Crisis*), a product of the Italian company Hacking Team [54]. We also located a structurally similar Word document via VirusTotal. The document used the same exploit and attempted to download a second stage from `rcs-demo.hackingteam.it`, which was unavailable at the time of testing.

Analysis of capabilities: RCS has a suite of functionality largely similar to FinSpy. One difference was in the vectors used to install the spyware. We located additional samples (see § 5), some of which were embedded in a `.jar` file that installs an OS-appropriate version of RCS (Windows or OSX), optionally using an exploit. If embedded as an applet, and no exploit is present, Java displays a security warning and asks the user whether they authorize the installation. We also saw instances of the **3-Stage Exploit Kit** where the first stage contained a Flash exploit; in some cases, we could obtain all stages and confirm that these installed RCS. Some samples were packed with the MPress packer [55], and some Windows samples were obfuscated to look like the `PuTTY` SSH client.

Another difference is in persistence. For example, the RCS sample sent to Ahmed adds a `Run` registry key, whereas the FinSpy samples used in Bahrain overwrite the hard disk's boot sector to modify the boot process; the spyware is loaded be-

fore the OS, and injects itself into OS processes as they start. The RCS samples we examined also had the ability to propagate to other devices, including into inactive VMWare virtual machines by modifying the disk image, onto USB flash drives, and onto Windows Mobile phones. We did not observe similar capabilities in the FinSpy samples we examined.

Exploitation of captured data: When Ahmed Mansoor received the RCS document, he opened it, infecting his computer (Figure 5). Ahmed subsequently noted several suspicious accesses to his GMail account using IMAP. Even after he changed his password, the accesses continued. While corresponding with Ahmed on his compromised account, an author of this paper discovered that the attackers had installed an *application-specific password* [56] in Ahmed's GMail account, a secondary password that they apparently used to access his account even after he changed his main password. The suspicious accesses stopped after removal of the application-specific password.

Two weeks after this correspondence with Ahmed, one of us (**Author** in Figure 5) received a targeted e-mail with a link to a file hosted on Google Docs containing a commercial off-the-shelf RAT, Xtreme RAT. The e-mail was sent from the UAE's timezone (as well as of other countries) and contained the terms "veryimportant" and "wikileaks", just like in the e-mail received by Ahmed.

The instance of Xtreme RAT sent to **Author** used `owner.no-ip.biz` for its C&C, one of the domains mentioned in a report published by Norman about a year-long campaign of cyberattacks on Israeli and Palestinian targets carried out by a group that Norman was unable to identify [57]. Three months after **Author** was targeted, Ahmed received an e-mail containing an attachment with Xtreme RAT that talked to the same C&C server (Figure 5), suggesting that the attackers who infected Ahmed with RCS may have provided a list of interesting e-mail addresses to another group for further targeting.

Possible consequences: Shortly after he was targeted, Ahmed says he was physically assaulted twice by an attacker who appeared able to track Ahmed's location [58]. He also reports that his car was stolen, a large sum of money disappeared from his bank account, and his passport was confiscated [59]. He believes these consequences are part of a government intimidation campaign against him, but we did not uncover any direct links to his infection. (Interestingly, spyware subsequently sent to others has used bait content about Ahmed.)

Further attacks: In October 2012, UAE **Journalist A** and **H**uman **R**ights **activist B** (per Figure 6) forwarded us suspicious e-mails they had received that contained a Word document corresponding to the first stage of **3-Stage Exploit Kit** (Figure 5). The attachment contained an embedded Flash file that exploited a vulnerability fixed in Adobe Flash 11.4, loading shell code to download a second stage from `faddeha.com`. We were unable to obtain the second stage or the ultimate payload, as the website was unavailable at the time of testing. However, the exploit kit appears indicative of Hacking Team involvement. A page on `faddeha.com` found in Google's cache contained an embedded `.jar` with the same applet class (*WebEnhancer*) as those observed in other `.jar` files that we found to contain RCS.

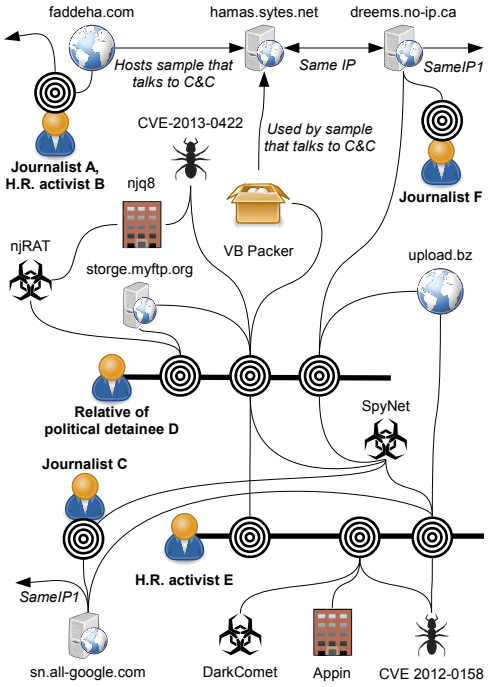


Figure 6: Another part of the ecosystem of UAE surveillance attacks.

Off-the-shelf RATs. We found a file that VirusTotal had downloaded from `faddeha.com`, which appeared to be a remote access toolkit known as *SpyNet*, available for general purchase for 50 Euros [60]. The SpyNet sample communicated with the C&C `hamas.sytes.net`.

SpyNet Packing: We found another instance of the first stage of the **3-Stage Exploit Kit** on VirusTotal. The exploit downloaded a second stage, which in turn downloaded a sample of SpyNet from `maile-s.com`. This sample of SpyNet communicated with the same C&C `hamas.sytes.net`. The sample was packed using *ASProtect* [61]. When run, the sample unpacks a compiled Visual Basic project that loads, via the `RunPE` method [62], an executable packed with *UPX* [63]. Finally, this executable unpacks SpyNet. SpyNet's GUI only offers an option to pack with UPX, suggesting that the attackers specially added the other layers of packing. In some cases, the Visual Basic project bears the name *NoWayTech*, which appears to be an underground `RunPE` tool, while others are named *SpyVisual*, which we have been unable to trace to any public underground tools, and thus also may reflect customization by the attacker. The *SpyVisual* projects contain the string `c:\Users\Zain\AppData\Local\Temp\OLE1EmbedStrm.wav`, which we used as the fingerprint **VB Packer** in Figure 6.

Cedar Key attack: The same **VB Packer** was used in an attack on **Relative of political detainee D** and **H.R. activist E** in Figure 6. These individuals received e-mails containing a link to a web page hosted on `cedarkeyrv.com` impersonating YouTube. Loading the page greeted the target with "*Video loading please wait ...*" The page redirected to a YouTube video a few seconds later, but first loaded a Java exploit [64]—a

known vulnerability with no patch at the time that the e-mails were sent. Oracle released a patch 12 hours after activists began receiving these links.

The cedarkeyrv.com domain is associated with an RV park in Cedar Key, Florida. The website's hosting company told us that the site had apparently suffered a compromise, but did not have further details.

The exploit used in the attack appears to have been originally posted by a Kuwaiti user, *njq8*, on an Arabic-language exploit sharing site [65]. We contacted *njq8*, who told us that he had obtained the exploit elsewhere and modified it prior to posting. The attack downloaded an instance of SpyNet from isteeler.com (which from our inspection did not appear to have any legitimate content), which used the C&C storge.myftp.org. This same C&C occurred in another attack (Figure 6) targeting **Relative of political detainee D**; in that case, the payload was a freely-available RAT known as *njRAT*, written by the same *njq8* as the exploit-poster discussed above. However, we did not find any other evidence suggesting *njq8*'s involvement in either attack.

More SpyNet attacks: The domain hamas.sytes.net, which we previously saw used by two SpyNet samples, resolved to 67.205.79.177. Historically, dreems.no-ip.ca also resolved to this address. An unidentified dropper using this C&C targeted **Journalist F**; a SpyNet attack on **Relative of political detainee D** also used this C&C. In that latter case, the sample arrived via e-mail in a .rar attachment that contained an .scr file disguised as a Word document. The .scr file was a self-extracting archive that decompressed and ran both the bait document and the payload. The SMTP source of the e-mail was webmail.upload.bz.

Appin: In early 2013 UAE **H.R. activist E** forwarded numerous documents that included a particular CVE-2012-0158 exploit for Microsoft Word. In all, these totaled 17 distinct hashes of documents, and 10 distinct hashes of payloads (some documents that differed in their hash downloaded the same payload). The exploits primarily downloaded instances of SpyNet from upload.bz, which for the most part communicated with C&C at sn.all-google.com. This domain was also used for C&C in other attacks, including that on **Journalist C**.

Two of the other CVE-2012-0158 exploits downloaded DarkComet from www.getmedia.us and www.technopenta.com after posting system information to random123.site11.com. All three domains match those used by an Indian cybermercenary group said to be linked to Appin Security Group [66]. The former two domains hosted content other than spyware (i.e., they may have been compromised). We alerted the owner of www.getmedia.us, who removed the payloads.

5 Empirical characterization

The samples we received afforded us an opportunity to empirically characterize the use of FinFisher and Hacking Team around the world, enabling us to assess their prevalence, and identify other country cases that may warrant future investigation. We analyzed the samples and the behavior of their C&C servers to develop indicators (fingerprints) for how the servers respond to certain types of requests. We then scanned the full Internet IPv4 address space ("/0") for these, along with probing results found by past scans. In many cases we do not release the full details of our fingerprints to avoid compromising what may be legitimate investigations.

5.1 FinSpy

Identifying and linking servers: We developed a number of fingerprints for identifying FinSpy servers using HTTP-based probing as well as FinSpy's custom TLV-based protocol. We leveraged quirks such as specific non-compliance with RFC 2616, responses to certain types of invalid data, and the presence of signatures such as the bizarre "Hallo Steffi" that Guarnieri identified from Bahraini FinSpy C&C servers [67, 68]. See Appendix A for details. We then exhaustively scanned the Internet looking for matches to these fingerprints.

Gamma documentation advertises that an operator of FinSpy can obscure the location of the C&C server (called the *master*) by setting up a proxy known as a *relay*. In Spring 2013 we noticed FinSpy servers now issuing 302 Redirects to google.com. However, we noticed anomalies: for example, servers in India were redirecting to the Latvian version of Google google.lv. We suspect that the server in India was a relay forwarding to a master in Latvia. Because the master served as a proxy for Google, we could uncover its IP address using a Google feature that prints a user's IP address for the query "IP address." We created an additional fingerprint based on the proxying behavior and issued GET /search?q=ip+address&nord=1 requests to servers We note some interesting master locations in Table 4.

Server locations: In all, our fingerprints matched 92 distinct IP addresses in 35 different countries. Probing these on 8/8/13 revealed 22 distinct addresses still responding, sited in: Bahrain, Bangladesh, Bosnia and Herzegovina, Estonia, Ethiopia, Germany, Hong Kong, Indonesia, Macedonia, Mexico, Romania, Serbia, Turkmenistan, and the United States. We found servers responding to a number of our fingerprints, suggesting either that some servers lag in their updates, or a concerted effort to vary the behavior of FinSpy servers to make detection harder.

We found: **(1)** 3 IP addresses in ranges registered to Gamma. **(2)** Servers in 3 IP ranges explicitly registered to government agencies: Turkmenistan's Ministry of Communications, Qatar's State Security Bureau, and the Bulgarian Council of Ministers. **(3)** 3 additional IP addresses in Bahrain, all in Batelco. **(4)** Servers in 7 countries with governments classified as "authoritarian regimes" by *The Economist* [69]: Bahrain, Ethiopia, Nigeria, Qatar, Turkmenistan, UAE, Vietnam.

Additional FinSpy samples: In parallel to our scanning, we obtained 9 samples of FinSpy by writing YARA [70] rules for the "malware hunting" feature of VirusTotal Intelligence. This feature sends us all newly-submitted samples that match our signatures. We located a version of FinSpy that does not use the normal FinSpy handshake, but instead uses a protocol based on HTTP POST requests for communication with the C&C server. This did not appear to be an older or newer ver-

Relay IP	Relay Block Assignment	Relay Country	Master IP	Master Block Assignment	Master Country
5.199.xxx.xxx	SynWebHost	Lithuania	188.219.xxx.xx	Vodafone	Italy
46.23.xxx.xxx	UK2 VPS.net	UK	78.100.xxx.xxx	State Security Building	Qatar
119.18.xxx.xxx	HostGator	India	81.198.xxx.xxx	Statoil DSL	Latvia
180.235.xxx.xxx	Asia Web Services	Hong Kong	80.95.xxx.xxx	T-Systems	Czech Republic
182.54.xxx.xxx	GPLHost	Australia	180.250.xxx.xxx	PT Telekom	Indonesia
206.190.xxx.xxx	WestHost	USA	112.78.xxx.xxx	Biznet ISP	Indonesia
206.190.xxx.xxx	Softlayer	USA	197.156.xxx.xxx	Ethio Telecom	Ethiopia
209.59.xxx.xxx	Endurance International	USA	59.167.xxx.xxx	Internode	Australia
209.59.xxx.xxx	Endurance International	USA	212.166.xxx.xxx	Vodafone	Spain

Table 4: Deproxifying FinSpy (mapping initial C&C IP addresses to the masters to which they forward).

sion of the protocol, suggesting that our scan results may not reveal the full scope of FinSpy C&C servers. Perhaps, the `HTTP POST` protocol was only delivered to a specific Gamma customer to meet a requirement.

5.2 Remote Control System (RCS)

We began by analyzing the UAE RCS sample from Ahmed and 6 samples obtained from VirusTotal by searching for AV results containing the strings "DaVinci" and "RCS." At the time, several AV vendors had added detection for RCS based on a sample analyzed by Dr. Web [71] and the UAE RCS sample sent to Ahmed. We also similarly obtained and analyzed samples of FSBSpy [72], a piece of malware that can report system information, upload screenshots, and drop and execute more malware, Based on these samples, we devised YARA signatures that yielded 23 additional samples of structurally similar malware.

Fingerprints: We probed the C&C servers of the RCS and FSBSpy samples, and found that they responded in a distinctive way to HTTP requests, and returned distinctive SSL certificates.

We searched sources including Shodan, 5 Internet Census service probes [73], and Critical.IO scanning data [68] for the observed distinctive HTTP behavior. We searched for the distinctive SSL certificates in two Internet Census service probes, and SSL certificate scans from ZMap [74]. We also contacted a team at TU Munich [75], who applied our fingerprints to their SSL scanning data. Across all of these sources, we obtained 31,345 indicator hits reflecting 555 IP addresses in 48 countries.

One SSL certificate returned by 175 of the servers was issued by "/CN=RCS Certification Authority /O=HT srl," apparently referring to the name of the spyware and the company. Servers for 5 of our FSBSpy samples and 2 of our RCS samples responded with this type of certificate.

Some servers returned these certificates in chains that included another distinctive certificate. We found 175 distinct IP addresses (including the C&C's for 5 of our FSBSpy samples and 2 of our RCS samples) responded with this second type of certificate.

We devised two more indicators: one that matched 125 IP addresses, including 7 of our FSBSpy samples' C&C's, and one that matched 2 IP addresses, in Italy and Kazakhstan.

Server locations: On 11/4/13 we probed all of the IP addresses that we collected, finding 166 active addresses matching one of our fingerprints in 29 different countries. We summarize the top providers and countries in Table 5.

Country	IPs
United States	61
United Kingdom	18
Italy	16
Japan	10
Morocco	7

Provider	IPs
Linode	42
NOC4Hosts	16
Telecom Italia	9
Maroc Telecom	7
InfoLink	6

Table 5: Top countries and hosting providers for RCS servers active on 11/4/13.

The prevalence of active servers either located in the USA or hosted by Linode is striking,[8] and seems to indicate a pervasive use of out-of-country web hosting and VPS services.

In addition, we found: **(1)** 3 IP addresses on a `/28` named "HT public subnet" that is registered to the CFO of Hacking Team [76]. The domain `hackingteam.it` resolves to an address in this range. **(2)** An address belonging to Omantel, a majority-state-owned telecom in Oman. This address was unreachable when we probed it; a researcher pointed us to an FSBSpy sample that contained an Arabic-language bait document about Omani poetry, which talked to a C&C in the UK. **(3)** 7 IP addresses belonging to Maroc Telecom. Moroccan journalists at Mamfakinch.com were previously targeted by RCS in 2012 [77]. **(4)** Overall, servers in 8 countries with governments deemed "authoritarian regimes" [69]: Azerbaijan, Kazakhstan, Nigeria, Oman, Saudi Arabia, Sudan, UAE, Uzbekistan.

Link to Hacking Team: All active servers matching one of our signatures also responded peculiarly when queried with particular ill-formed HTTP requests, responding with "`HTTP1/1 400 Bad request`" (should be "`HTTP/1.1`") and a body of "`Detected error: HTTP code 400`". Googling for this response yielded a GitHub project `em-http-server` [78], a Ruby-based webserver. The project's author is listed as Alberto Ornaghi, a software architect at Hacking Team. We suspect that the Hacking Team C&C server code may incorporate code from this project.

Links between servers: We identified many cases where several servers hosted by different providers, and in different countries, returned identical SSL certificates matching our fingerprints. We also observed 30 active servers used a global IPID. Only one active server had neither a global IPID nor

[8] 19 of the 42 Linode servers were hosted in the USA, so the two patterns of prevalence are mostly distinct.

an SSL certificate matching our fingerprints. We assessed whether servers returning SSL certificates were forwarding to the servers with global IPIDs by inducing bursts of traffic at the former and monitoring the IPID at the latter. For 11 servers, we found that the server's activity correlated to bursts sent to other servers We grouped servers by the SSL certificates they returned, and found that each group forwarded to only a single server, except for one case where a group forwarded to two different IPs (both in Morocco). We also found two groups that forwarded to the same address. There was a 1:1 mapping between the remaining 8 addresses and groups. We refer to a group along with the server(s) it forwards to as a *server group*. We identified several server groups that may be associated with victims or operators in a certain country. Some of these suggest possible further investigation:

Turkey: We identified a group containing 20 servers in 9 countries. Two RCS and 5 FSBSpy samples from VirusTotal communicated with various servers in the group. The RCS samples also communicated with domains with lapsed registrations, so we registered them to observe incoming traffic. We exclusively received RCS traffic from Turkish IP addresses. (RCS traffic is identifiable based on a distinctive user agent and URL in `POST` requests.) A sample of FSBSpy apparently installed from an exploit on a Turkish server talked to one of the servers in this group.[79]

We also found server groups containing servers in **Uzbekistan** and **Kazakhstan**; we found FSBSpy samples on VirusTotal uploaded from these countries that communicated with servers in these groups.

In the above cases, save Turkey, the country we have identified is classified as an "authoritarian regime," and may be using Hacking Team products against the types of targets we profile in this paper. In the case of Turkey, there are hints that the tool may be employed against dissidents [80].

6 Summary

Targeted surveillance of individuals conducted by nation-states poses an exceptionally challenging security problem, given the great imbalance of resources and expertise between the victims and the attackers. We have sketched the nature of this problem space as reported to us by targeted individuals in three Middle Eastern countries. The attacks include spyware for ongoing monitoring and the use of "IP spy" links to deanonymize those who voice dissent.

The attacks, while sometimes incorporating effective social engineering, in general lack novel technical elements. Instead, they employ prepackaged tools developed by vendors or acquired from the cybercrime underground. This technology sometimes suffers from what strike us as amateurish mistakes (multiple serious errors implementing cryptography, broken protocol messages), as does the attackers' employment of it (identifying-information embedded in binaries, C&C servers discoverable via scanning or "Google hacking", clusters of attack accounts tied by common activity). Some of these errors assisted our efforts to assemble strong circumstantial evidence of governmental origins. In addition, we mapped out the global use of two "governmental" hacking suites, including identifying 11 cases in which they appeared to be used in countries governed by "authoritarian regimes."

We aim with this work to inspire additional research efforts addressing the difficult problem of how to adequately protect individuals with very limited resources facing very powerful adversaries. Open questions include robust, practical detection of targeted attacks designed to exfiltrate data from a victim's computer, as well as detection of and defense against novel attack vectors, like tampering with Internet connections to insert malware.

The task is highly challenging, but the potential stakes are likewise very high. An opposition member, reflecting on government hacking in Libya, speculated as to why some users would execute files even while recognizing them as potentially malicious [2]: "*If we were vulnerable we couldn't care less … we were desperate to get our voices out … it was a matter of life or death … it was just vital to get this information out.*"

Acknowledgment

This work was supported by the National Science Foundation under grants 1223717 and 1237265, and by a Citizen Lab Fellowship. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

The authors would like to thank the following individuals for their help in various aspects of our analysis: Bernhard Amman, Collin D. Anderson, Brandon Dixon, Zakir Durumeric, Eva Galperin, Claudio Guarnieri, Drew Hintz, Ralph Holz, Shane Huntley, Andrew Lyons, Mark Schloesser, and Nicholas Weaver.

References

[1] "Dark Secrets—Hacking Team commercial," accessed: 12-November-2013. [Online]. Available: http://bit.ly/1bCh57v

[2] J. Scott-Railton, "Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution," US Naval War College, Tech. Rep., 2013.

[3] S. H. AlJalahma, "Response to The Guardian—UK companys software used against Bahrain activist," May 2013, accessed: 12-November-2013. [Online]. Available: http://bit.ly/19iVUUP

[4] V. Silver, "Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy," Jul. 2012, accessed: 12-November-2013. [Online]. Available: http://bloom.bg/17SOXQs

[5] A. Jeffries, "Meet Hacking Team, the company that helps the police hack you," Sep. 2013, accessed: 12-November-2013. [Online]. Available: http://bit.ly/1bCajyl

[6] T. Brewster, "From Bahrain To Belarus: Attack Of The Fake Activists," Jul. 2013, accessed: 12-November-2013. [Online]. Available: http://bit.ly/1gIgwhW

[7] V. Silver, "MJM as Personified Evil Says Spyware Saves Lives Not Kills Them," 2011, accessed: 12-November-2013. [Online]. Available: http://bloom.bg/170E8sQ

[8] D. Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," 2013, accessed: 12-November-2013. [Online]. Available: http://bit.ly/17tBBtm

[9] R. Clayton, S. J. Murdoch, and R. N. Watson, "Ignoring the Great Firewall of China," in *PETS*. Springer, 2006, pp. 20–35.

[10] J. R. Crandall et al., "ConceptDoppler: A Weather Tracker for Internet Censorship," in *ACM CCS*, 2007.

[11] X. Xu, Z. M. Mao, and J. A. Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" in *Proc. PAM*, 2011.

[12] M. Sherr, G. Shah, E. Cronin, S. Clark, and M. Blaze, "Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps," in *ACM CCS*, 2009, pp. 512–523.

[13] J. R. Crandall, M. Crete-Nishihata, and J. Knockel, "Chat program censorship and surveillance in China: Tracking TOM-Skype and Sina UC," *First Monday*, vol. 18, no. 7, Jul. 2013, accessed: 8-August-2013. [Online]. Available: http://bit.ly/1fzNcHl

[14] S. Wolchok, R. Yao, and J. A. Halderman, "Analysis of the Green Dam Censorware System," Tech. Rep., 2009.

[15] F. Li, A. Lai, and D. Ddl, "Evidence of Advanced Persistent Threat: A case study of malware for political espionage," in *MALWARE*, 2011.

[16] "Default https access for Gmail," 2010, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1bBktPM

[17] "Making Twitter more secure: HTTPS," 2011, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1i7l9kM

[18] L. Constantin, "Facebook to roll out HTTPS by default to all users," 2012, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1bsLBCm

[19] "FinFisher: Governmental IT Intrusion and Remote Monitoring Solutions," accessed: 12-November-2013. [Online]. Available: http://bit.ly/1840Lxn

[20] "BlackBerry rogue software leaves sour taste in UAE," 2013, accessed: 11-November-2013. [Online]. Available: http://on.ft.com/HVXvJP

[21] Mandiant, "The Advanced Persistent Threat," 2010.

[22] ——, "APT1: Exposing One of China's Cyber Espionage Units," 2013.

[23] S. Fagerland, M. Krakvik, J. Camp, and N. Moran, "Operation Hangover: Unveiling an Indian Cyberattack Infrastructure," 2013.

[24] R. Deibert and R. Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, p. 6, 2009.

[25] S. Nagaraja and R. Anderson, "The snooping dragon: social-malware surveillance of the Tibetan movement," Tech. Rep., 2009.

[26] F. C. Solutions, ""njRAT" Uncovered," 2013, accessed: 25-June-2013. [Online]. Available: http://bit.ly/1eJheel

[27] "FinFisher - Excellence in IT Investigation," accessed: 27-February-2014. [Online]. Available: http://www.finfisher.com/

[28] R. Rolles, "Unpacking virtualization obfuscators," in *USENIX WOOT*, 2009.

[29] "TEMU: The BitBlaze Dynamic Analysis Component," accessed: 7-August-2013. [Online]. Available: http://bit.ly/1clcxSZ

[30] "'Reinstate sacked official' call," 2013, accessed: 11-November-2013. [Online]. Available: http://bit.ly/1aRUZ4b

[31] "Unionist Questioned," 2013, accessed: 23-April-2013. [Online]. Available: http://bit.ly/1gHnBiS

[32] N. Villeneuve, "Fake Skype Encryption Service Cloaks DarkComet Trojan," Apr. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/17SpA1c

[33] E. Galperin and M. Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Mar. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/HSCRet

[34] ——, "New Wave of Facebook Phishing Attacks Targets Syrian Activists," Apr. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/1hDQsG8

[35] ——, "Pro-Syrian Government Hackers Target Activists With Fake Anti-Hacking Tool," Aug. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/1eJj12T

[36] J. Scott-Railton and M. Marquis-Boire, "A Call to Harm: New Malware Attacks Target the Syrian Opposition," Citizen Lab, Tech. Rep., Jun. 2013, accessed: 3-August-2013. [Online]. Available: http://bit.ly/1a2l9PK

[37] E. Galperin and M. Marquis-Boire, "Trojan Hidden in Fake Revolutionary Documents Targets Syrian Activists," May 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/1cSJT0

[38] M. Marquis-Boire and S. Hardy, "Syrian Activists Targeted with BlackShades Spy Software," Jun. 2012, accessed: 12-November-2013. [Online]. Available: http://bit.ly/1a2l6mX

[39] S. Fagerland, "The Syrian Spyware," Feb. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/HLyGR9

[40] Telecomix, "REPORT of a Syrian spyware," p. 9, Feb. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/1bsNcIk

[41] S. Faris, "The Hackers of Damascus," Nov. 2012, accessed: 9-August-2013. [Online]. Available: http://buswk.co/17t8RRH

[42] L. Aylward, "Malware Analysis—Dark Comet RAT," Nov. 2011, accessed: 4-August-2013. [Online]. Available: http://bit.ly/16ZXgag

[43] Quequero, "DarkComet Analysis—Understanding the Trojan used in Syrian Uprising," Mar. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/19i6kEl

[44] S. Denbow and J. Hertz, "Pest Control: Taming the RATs," p. 14, accessed: 12-November-2013. [Online]. Available: http://bit.ly/1fzLA0m

[45] B. Brumfield, "Computer spyware is newest weapon in Syrian conflict," Feb. 2012, accessed: 4-August-2013. [Online]. Available: http://cnn.it/HLz5TA

[46] "jalnosra.com," accessed: 27-February-2014. [Online]. Available: jalnosra.com

[47] "Skype Encryption.wmv," accessed: 27-February-2014. [Online]. Available: http://bit.ly/HZ3e1y

[48] E. Galperin and M. Marquis-Boire, "The Internet is Back in Syria and So is Malware Targeting Syrian Activists," Dec. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/1bngqFc

[49] "Free Syrian Army Sex Tape—Abdul Razzaq Tlass [NSFW]," accessed: 5-August-2013. [Online]. Available: http://bit.ly/1gHqDDH

[50] A. Lund, "Holy Warriors: A field guide to Syria's jihadi groups," Oct. 2012, accessed: 5-August-2013. [Online]. Available: http://atfp.co/17t8yq5

[51] "Ahmed Mansoor and Four Other Pro-Democracy Activists Pardoned and Freed," 2013, accessed: 10-November-2013. [Online]. Available: http://bit.ly/18pHpis

[52] "Royal Group," accessed: 27-February-2014. [Online]. Available: http://www.royalgroupuae.com/

[53] T. Katsuki, "Crisis for Windows Sneaks onto Virtual Machines," 2012, accessed: 27-February-2014. [Online]. Available: http://bit.ly/MzheRJ

[54] "Hacking Team," accessed: 27-February-2014. [Online]. Available: http://www.hackingteam.it/

[55] "MPRESS," accessed: 27-February-2014. [Online]. Available: http://www.matcode.com/mpress.htm

[56] "Sign in using application-specific passwords," accessed: 27-February-2014. [Online]. Available: https://support.google.com/accounts/answer/185833?hl=en

[57] S. Fagerland, "Systematic cyber attacks against Israeli and Palestinian targets going on for a year," 2012, accessed: 12-November-2013. [Online]. Available: http://bit.ly/1aSdw07

[58] V. Silver, "Spyware Leaves Trail to Beaten Activist Through Microsoft Flaw," 2012, accessed: 14-November-2013. [Online]. Available: http://bloom.bg/1ja2geI

[59] B. Hubbard, "Emirates Balk at Activism in Region Hit by Uprisings," 2013, accessed: 14-November-2013. [Online]. Available: http://nyti.ms/I4n2Aw

[60] "SPY NET," accessed: 27-February-2014. [Online]. Available: http://newspynetrat.blogspot.com/

[61] "Asprotect SKE," accessed: 27-February-2014. [Online]. Available: http://www.aspack.com/asprotect32.html

[62] "Unpacking VBInject/VBCrypt/RunPE," 2010, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1e28nS2

[63] "Ultimate Packer for eXecutables," accessed: 27-February-2014. [Online]. Available: http://upx.sourceforge.net/

[64] "CVE-2013-0422," accessed: 27-February-2014. [Online]. Available: http://bit.ly/NA1O0A

[65] njq8, "New java drive-by 2013-1-11," 2013, accessed: 27-February-2014. [Online]. Available: http://www.devpoint.com/vb/t357796.html

[66] "Appin Technology Lab," accessed: 27-February-2014. [Online]. Available: http://www.appinonline.com/

[67] C. Guarnieri, "Analysis of the FinFisher Lawful Interception Malware," 2012, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1eJjVMV

[68] H. Moore, "Critical Research: Internet Security Survey," 2012.

[69] "Democracy Index 2012: Democracy at a Standstill," 2012, accessed: 7-August-2013. [Online]. Available: http://bit.ly/HSEDMD

[70] "YARA - The pattern matching swiss knife for malware researchers," accessed: 27-February-2014. [Online]. Available: http://plusvic.github.io/yara/

[71] "Cross-platform Trojan controls Windows and Mac machines," 2012, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1eJnJgZ

[72] S. Golovanov, "Adobe Flash Player 0-day and HackingTeam's Remote Control System," 2013, accessed: 7-August-2013. [Online]. Available: http://bit.ly/17n12ro

[73] "Internet Census 2012," 2013, accessed: 7-August-2013. [Online]. Available: http://bit.ly/1i7rRHs

[74] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-Wide Scanning and its Security Applications," in *USENIX Security*, Aug. 2013.

[75] "Home of Crossbear and OONIBear," accessed: 27-February-2014. [Online]. Available: https://pki.net.in.tum.de/

[76] "RIPE Database Query for FASTWEB-HT," accessed: 27-February-2014. [Online]. Available: http://bit.ly/MzkigV

[77] "How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists," 2012, accessed: 7-August-2013.

[78] A. Ornaghi, "em-http-server," accessed: 27-February-2014. [Online]. Available: https://github.com/alor/em-http-server

[79] SophosLabs, "Anatomy of a targeted attack—SophosLabs explores an Adobe zero-day "malware experiment"," 2013, accessed 7-August-2013. [Online]. Available: http://bit.ly/HQ1oRc

[80] K. Zetter, "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments," 2013, accessed: 14-November-2013. [Online]. Available: http://wrd.cm/1fHonth

[81] M. Marquis-Boire and B. Marczak, "From Bahrain With Love: FinFisher's Spy Kit Exposed?" Jul. 2012, accessed: 4-August-2013. [Online]. Available: http://bit.ly/1bngpB2

A FinSpy fingerprints

Previous work by Guarnieri on scanning for FinSpy servers found that in response to a request such as `GET /`, the Bahraini FinSpy C&C server returns a response with the string "`Hallo Steffi`" [67]. Guarnieri searched a database of such responses compiled by the Critical.IO Internet scanning project [68], locating 11 additional servers in 10 countries [67]. We refer to this fingerprint as α_1. Concurrent with this effort, we devised our own fingerprint β_1 that tested three aspects of the handshake between a FinSpy infectee and a FinSpy C&C server, which follows a custom TLV-based protocol running on ports such as 22, 53, 80, and 443. We conducted targeted scanning of several countries using β_1, and also confirmed Guarnieri's findings for those servers still reachable after he published his findings.

We observed a trend: changes in HTTP response behavior by FinFisher after publication of findings about the software. In July 2012, for example, after a post about Bahraini FinSpy samples [81], servers closed the TCP connection in response to a `GET /` or `HEAD /` request (although servers continued to behave consistently with β_1. Other changes followed later in 2012, including a new response to `GET /` requests that included an imperfect copy of an Apache server's HTTP response (the `Date` header used `UTC` rather than `GMT`). We fingerprinted this error as α_2, and later in 2012 fingerprinted other distinctive behavior in response to `GET /` requests as α_3.

Subsequent scans of `/0` for α_2 and α_3, and five service probes of the Internet Census for α_1 through α_3, located several additional servers. In Feburary 2013 we identified and fingerprinted new HTTP response behavior with α_4 and modified β_1 to produce β_2, which tests only two of the three aspects of the FinSpy handshake (the third test of β_1 was broken when FinSpy servers were updated to accept types of invalid data they had previously rejected).

As of 3/13/13, all servers that matched any α fingerprint matched β_2.