



Gift Cardsharks: The Massive Threat Campaigns Circling Beneath the Surface

Authors: Yonathan Klijnsma & Steve Ginty



Table of Contents

Foreword	3
Executive Summary.....	4
Timeline	6
Targets	8
Financial Transactions Processing, Reserve, and Clearinghouse Activities	8
Information Technology	9
Retail, Restaurants, & Travel	9
Employee Rewards and Corporate Loyalty	10
Digital Marketing & Communications	10
Unknown.....	10
Targeting Hypotheses	11
Methods of Operation.....	12
Phishing Pages.....	12
Connections to the Lucy Phishing Platform.....	13
Lucy Headers.....	15
Lucy Phishing Templates	15
Digital Marketing for Phishing Delivery, Tracking, & Analytics	18
Implants & Tools	20
Legitimate Tools	20
PowerShell.....	21
BabySharkPro.....	21
Empire: Get-Keystores	22
Staging of payloads	23
Infrastructure	24
Hosting Providers.....	24
SSL Certificate Usage and Overlap	25
Domain Registrants	27
Jacob Rummel.....	27
Ivan Wilshea.....	28
Conclusion	30
Indicators of Compromise (IOCs).....	31

Foreword

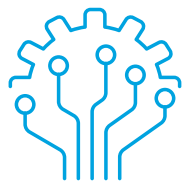
Over the past several weeks, various elements of a more substantial breach of IT supplier Wipro has become public.

Investigative journalist Brian Krebs [first reported](#) the attack on his website “Krebs on Security,” which explained how Wipro’s IT systems were compromised and used to attack the company’s customers. After contacting Wipro, Krebs followed up on his article by publishing updates on the breach. While Wipro was generally close-lipped on the incident, some of the victims breached through Wipro spoke with him and provided Indicators of Compromise (IOCs) they uncovered. Krebs proceeded to publish this small set of IOCs on his website.

However, Wipro was far from the first company to be compromised by this campaign and was only one of a long list of targets dating back to 2016. While a spotlight was shone on this attack due to the high visibility of Wipro, we’ve written this report to shed light on the far more critical story around this attacker:

- This campaign goes far beyond Wipro
- The sophisticated, highly targeted nature of their attacks
- The sheer breadth of their targets
- The widely available tools they used to execute their attacks and feign legitimacy
- Their unique monetization techniques leveraging gift card infrastructure

Executive Summary



Using our vast collection grid and unique external view of threat actor operations, RiskIQ can piece together a more complete picture of this actor group and their attack campaigns, tools, and possible motives. This report is by no means a comprehensive analysis but builds a detailed narrative of widely-reported events.



The actors in this attack have been operating since mid-2016, and analysis of their targets, based on companies included in their phishing domains, indicates that the actors were primarily targeting major gift card retailers, distributors, and card processors. As a result, we believe gaining access to gift card infrastructure was part of a unique monetization process and indicates that their motives may be financial.



These attacks followed a roughly consistent kill chain. To create effective email phishing campaigns and appear legitimate to targets' network security, they leveraged widely used email marketing and analytics tools. These phishing emails targeted retailers, employee reward programs, and many other organizations dealing in gift cards. With access to this gift card infrastructure, the attackers went on to use money transfer services, clearinghouses, and other payment processing institutions to monetize.



The actors appear to utilize commercially available and open-source software, including, ironically, platforms meant to train employees in phishing prevention, along with PowerShell to steal credentials and certificates to use toward broader reach. One of these PowerShell scripts, BabySharkPro (to which we allude in the title of this report), is often associated with North Korean threat activity, but this may have been a false flag put in place by the actors to mislead researchers.



We believe subsequent attacks on IT infrastructure organizations like Wipro and several others represented broader targeting by the threat group in an attempt to widen its reach.



Infrastructure overlap in PDNS, WHOIS, and SSL certificate data sets allowed RiskIQ to build out a more comprehensive understanding of actor-owned infrastructure, possible targets, and a timeline of the attack campaigns. This report is an analysis of these campaigns, their operators, and their targets.

Timeline

RiskIQ has identified at least five distinct attack campaigns based off analysis of the actor-owned infrastructure. We built this timeline with both Passive DNS and SSL Certificate data collected by RiskIQ technology. In most instances, the attackers targeted an organization for only a short period, allowing their phishing pages to be up for just one or two days after they sent out their malicious emails. After this time, the server stopped responding for the phishing hostnames, and we no longer observed DNS resolutions for them.

The first campaign appears to have started in May of 2016 and continued through August of 2016. During this initial attack campaign, the actors' targets are as follows:

Eight companies across the below industries over four months:

- Retail Organizations
- Digital Marketing / Marketing Automation
- Employee Rewards Providers
- Customer Loyalty & Recognition
- Gift Card providers
- Information Technology

The second campaign was active from February 2017 - March of 2017 and retargeted four of the same companies initially targeted during the 2016 campaign:

- Gift Card Providers
- Employee Rewards Providers
- Customer Loyalty & Recognition

Actors launched a third campaign on November 2017 targeting four new organization (one a subsidiary of a previous target) across the following industries:

- Payment Transfer Services
- Point of Sale, Prepaid Services, Money Transfer
- Information Technology (online fax service)

The actors' fourth attack campaign started in February of 2018 and continued through May of 2018. Actors targeted 23 companies overall, including seven organizations they had previously targeted.

The following industries were targeted:

- Retail
- Digital Marketing / Marketing Automation
- Loyalty Rewards
- Gift Card providers
- Information Technology
- Payment Transfer Services
- Point of Sale, Prepaid Services, Money Transfer
- Payment Services
- Travel Platforms

The actors 5th campaign took place between January 2019 - May 2019. This campaign is the most well known and the one associated with the Wipro breach. This campaign significantly expanded the groups targeting list and included a larger focus on IT outsourcers, consultants, and managed service providers.

Actors targeted 24 organizations

- 7 previous targets
- 17 New organizations

The following industries were targeted:

- Retail
- Digital Marketing / Marketing Automation
- Loyalty Rewards Companies
- Gift Card providers
- Information Technology
- Payment Transfer Service
- Point of Sale, Prepaid Services, Money Transfer
- Payment Services
- Travel Platforms

Targets

Our target analysis is based on the fact that the actors used fully qualified domain names (FQDNs) with the target organization name or domain. While we can determine organizations of interest to this actor group based on infrastructure, a target does not imply a victim or that the actor group was successful in breaching the organization.

Our analysis of the infrastructure used in the attack campaigns led us to determine that this actor group is targeting the following industries/verticals:

Financial Transactions Processing, Reserve, and Clearinghouse Activities

Company	Website	Headquartered
Greendot Corporation	https://www.greendot.com/	United States
Wolfe	https://www.wolfe.com/	United States
Blackhawk Networks	http://www.blackhawknetwork.com/	United States
CashStar (Blackhawk Networks)	https://www.cashstar.com/	United States
Paysafe Group	https://www.paysafe.com/na-en/	Isle of Man
Incomm	https://www.incomm.com/	United States
Euronet Worldwide	https://www.euronetworldwide.com/	United States
MoneyGram	https://secure.moneygram.com/mgo/us/en/	United States
UAE Exchange	https://www.uaeexchange.com/	United Arab Emirates
Western Union	https://www.westernunion.com/us/en/home.html	United States
WorldRemit	http://www.worldremit.com/	United Kingdom
Sigue	https://sigue.com/	United States
First Data	https://www.firstdata.com/en_us/home.html	United States
Comdata	http://www.comdata.com/	United States
Stored Value (Comdata)	http://www.storedvalue.com/en-US/home	United States
Fleetcor	http://www.fleetcor.com/	United States
Elavon	https://www.elavon.com/	United States

Information Technology

Company	Website	Headquartered
Rackspace	https://www.rackspace.com/	United States
ServiceNow	https://www.servicenow.com/	United States
Avande (Accenture)	https://www.avande.com/en-us	United States
PCM	http://www.pcm.com/	United States
Cognizant	https://www.cognizant.com/	United States
Capgemini	http://www.capgemini.com/	France
Infosys	http://www.infosys.com/	India
Wipro	https://www.wipro.com/en-US/	India
Slalom	https://www.slalom.com/	United States
GFI Software	https://www.gfi.com/	Malta

Retail, Restaurants, & Travel

Company	Website	Headquartered
Best Buy	https://www.bestbuy.com/	United States
Sears Holdings	https://searsholdings.com/	United States
Staples	https://www.staples.com/	United States
Costco	https://www.costco.com/	United States
Gamestop	https://www.gamestop.com/	United States
Darden Restaurants	https://www.darden.com/	United States
Card Cash	https://cardcash.com/	United States
eGifter	https://www.egifter.com/	United States
Outerwall / Coinstar	https://www.coinstar.com/	United States
Expedia Group	http://www.expediagroup.com/	United States
Booking Holdings	https://www.bookingholdings.com/	United States
Agoda (Booking Holdings)	http://www.agoda.com/	Singapore

Employee Rewards and Corporate Loyalty

Company	Website	Headquartered
Affinion Group	http://www.affinion.com/	United States
O.C. Tanner	https://www.octanner.com/	United States
Bridge2 Solutions	http://www.bridge2solutions.com	United States
Achievers (Blackhawk Networks)	https://www.achievers.com/	United States
Globoforce / Workhuman	https://www.globoforce.com/company/	United States
Virgin Pulse	https://www.virginpulse.com/	United Kingdom
ITA Group	https://www.itagroup.com/	United States

Digital Marketing & Communications

Company	Website	Headquartered
SmartFocus	https://www.smartfocus.com/en	United States
InsideView	http://www.insideview.com/	United States
Dotdigital	https://dotdigital.com/	United Kingdom
SendGrid	https://sendgrid.com/	United States
Act-On	https://www.act-on.com/	United States
MessageLab	https://www.messagelab.com/	United States
Episerver	https://episerver.com	United States
Infogroup	http://www.infogroup.com/	United States
ZoomInfo	http://www.zoominfo.com/	United States

Unknown

There is also a large pool of unknown targets and victims. Unlike most of the phishing attacks in this campaign, the infrastructure used to target these unknown targets did not include the organization's name so we could not identify them.

Targeting Hypotheses

Analysis of the targeted organizations across all attack campaigns highlights a few common threads:

- Traditional retail organizations are significant targets
 - Example targets: Best Buy, Sears, Darden Foods, Costco,
 - A possible theory for targeting could be that gift cards provide access to liquid assets outside of the traditional western financial system
- Company and employee rewards programs
 - Example targets: Affinion Group, O.C. Tanner, Achievers
 - Possible targeting theory: Most of these rewards programs offer broad access to gift card based rewards
- Gift card providers and processors
 - Example targets: Incomm, Greendot, BlackHawk Networks, Wolfe
 - Possible targeting theory: Actors need a way to convert gift cards into currency and effectively transfer funds to more traditional institutions
- Digital marketing and marketing automation firms
 - Example targets: SmartFocus, Insideview, SendGrid, Socialab
 - Possible targeting theory: Actors can leverage these platforms and services for distribution of their phishing emails
 - RiskIQ has observed some of the above services being used in conjunction with the actors' attacks
- Information Technology
 - Example targets: Rackspace, Wipro, Infosys, PCM
 - A possible theory for targeting is that Rackspace is a major cloud provider for Financial services and organizations. Actors could be looking to target the third-party provider to compromise multiple organizations.

Additional targeting highlights:

- The actors focused on traditional Retail targets in their initial 2016 attack campaign.

- They expanded targeting in their 2017 attack campaigns to include organizations' employee rewards and corporate loyalty programs which may indicate they needed a broader collection of targets
- Travel platforms such as Agoda and Expedia are added to their expanded targeting list in 2018
- Outside of initial targeting of Rackspace, the threat actors do not expand targeting to include additional information technology organizations until their now infamous 2019 campaign against Wipro.

Methods of Operation

To create effective email phishing campaigns and appear legitimate to targets' network security and anti-phishing tools, the attackers leveraged widely used email marketing and analytics tools. These phishing emails targeted organizations dealing in gift cards such as retailers and human resources platforms, using relatively generic templates and switching out the logo and branding to reflect the target organization.

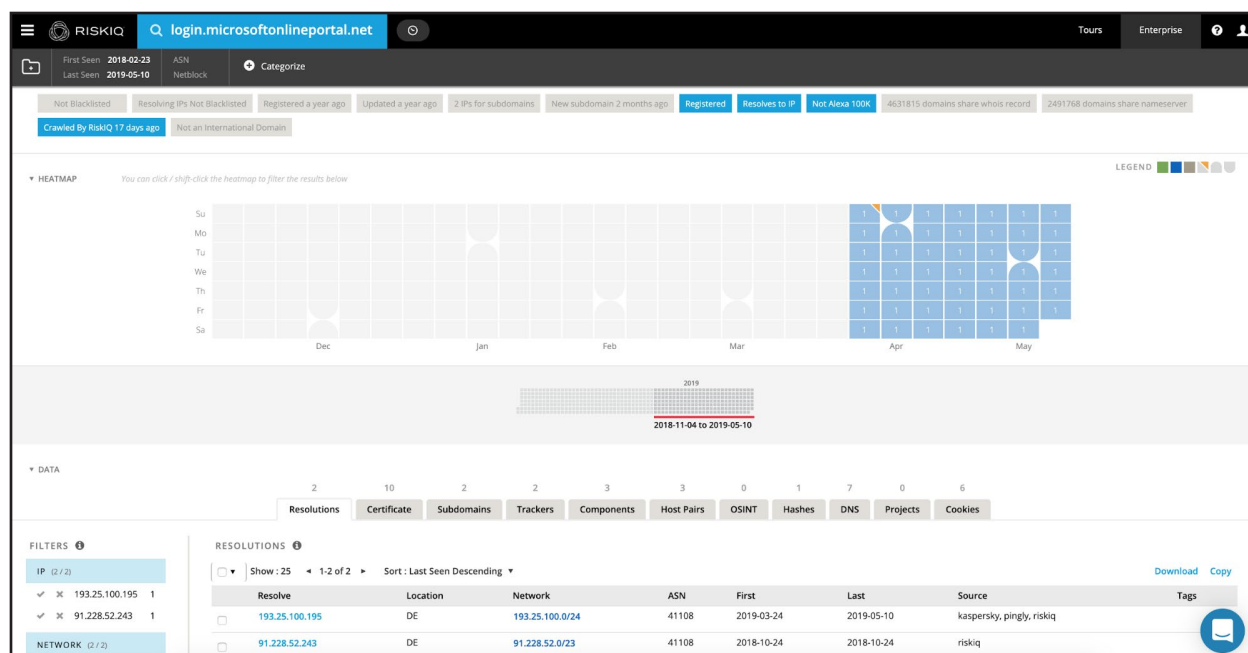
Phishing Pages

The attackers used phishing pages to attack their targets. These pages have reasonably generic login forms, and would all be similar except for the names of the targeted organizations. The attackers did not create these phishing page designs or the system that serves them themselves—they made use of a phishing software package called Lucy, which allowed them to automate much of the work.

When RiskIQ crawlers visit websites, they record all resources and add them to an index of every resource we've ever seen and where we've seen it. We discovered the attackers' usage of Lucy when we compared the phishing pages used in the different campaigns and noticed a lot of shared resources. When we compared hosts returning the same resources, many were using Lucy, adding Lucy as a new web component on which to search for more of this phishing infrastructure.

Connections to the Lucy Phishing Platform

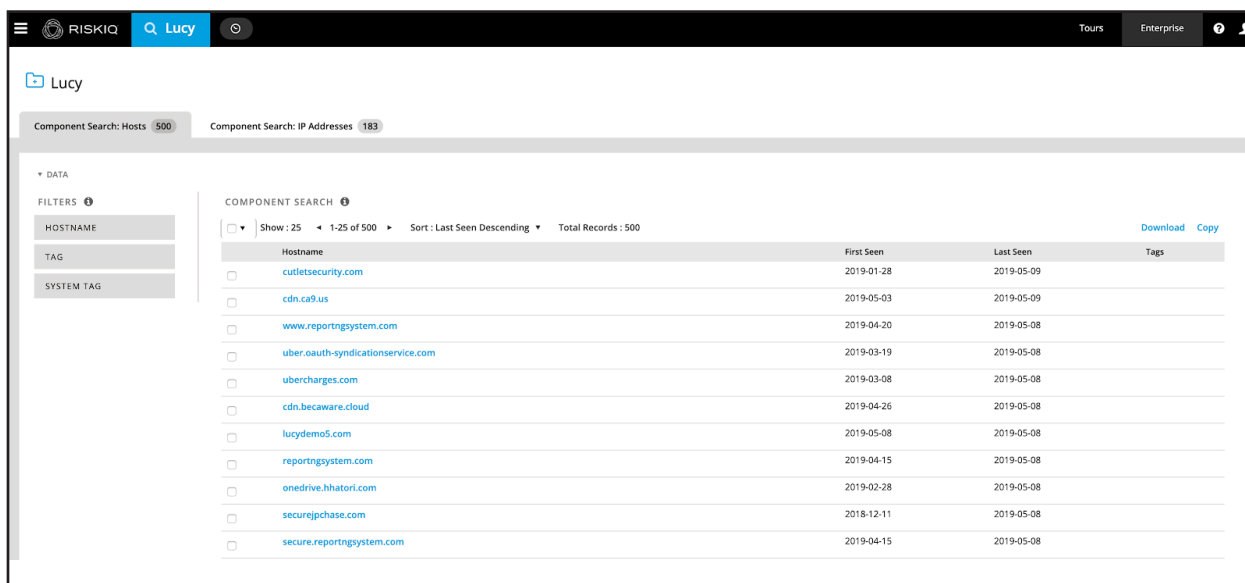
Analyzing one of the javascript files (detect.js) associated with the actors' fishing campaign, led RiskIQ analysts to uncover three additional URLs related to the same file. One of the hosts login[.]microsoftonlineportal[.]net - was of particular interest as it appeared similar to the actors' domain registration structure.



<https://community.riskiq.com/search/login.microsoftonlineportal.net>

Investigating the domain's resolution history unveiled IP addresses with significant typosquatting domains registered that appeared to be targeting European corporations. Additional analysis of RiskIQ's component data set revealed a unique server association for the domains in question: Lucy.

A query of our RiskIQ's component database as of May 9th shows 500 hosts and 183 IP addresses with that server component present:



Component Search: Hosts 500 Component Search: IP Addresses 183

DATA

FILTERS

HOSTNAME

TAG

SYSTEM TAG

COMPONENT SEARCH

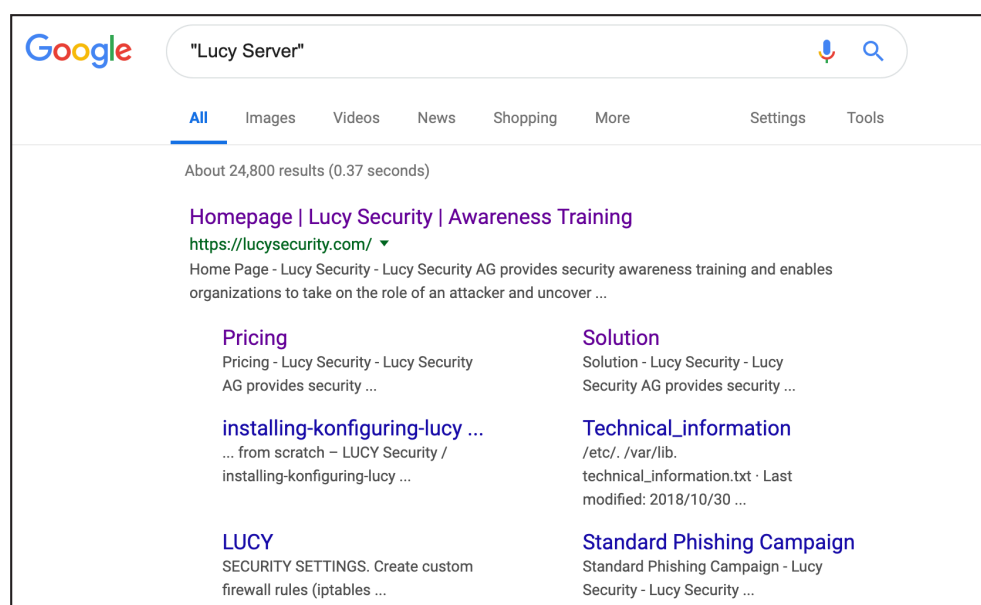
Show: 25 1-25 of 500 Sort: Last Seen Descending Total Records: 500

Hostname	First Seen	Last Seen	Tags
cutletsecurity.com	2019-01-28	2019-05-09	
cdn.ca9.us	2019-05-03	2019-05-09	
www.reportingssystem.com	2019-04-20	2019-05-08	
uber.oauth-syndication-service.com	2019-03-19	2019-05-08	
ubercharges.com	2019-03-08	2019-05-08	
cdn.becaware.cloud	2019-04-26	2019-05-08	
lucydemo5.com	2019-05-08	2019-05-08	
reportingsystem.com	2019-04-15	2019-05-08	
onedrive.khatori.com	2019-02-28	2019-05-08	
securejpcase.com	2018-12-11	2019-05-08	
secure.reportingssystem.com	2019-04-15	2019-05-08	

Download Copy

<https://community.riskiq.com/search/components/Lucy>

Running a Google search for the phrase “Lucy Server” revealed a possible connection to a security company based in Zug Switzerland that offers a SaaS phishing platform for organizations to conduct security and phishing awareness training:



Lucy Headers

RiskIQ crawlers identified a server installation called Lucy, which shows in the server header of certain Lucy installations. One interesting thing to note is that whether or not you see this header depends on how you install Lucy. In general, it comes down to these installation methods:

- Preconfigured Virtual Machine: Shows Lucy server header
- Manual installation through a script: Does not show Lucy server header

The attackers performed manual installations of their Lucy servers every time, which means only the Apache headers show most of the time, with Nginx showing some of the time.

Lucy Phishing Templates

Lucy comes with a variety of default phishing templates, and one of these templates was used during most of the phishing campaigns—including the now notorious Wipro case:



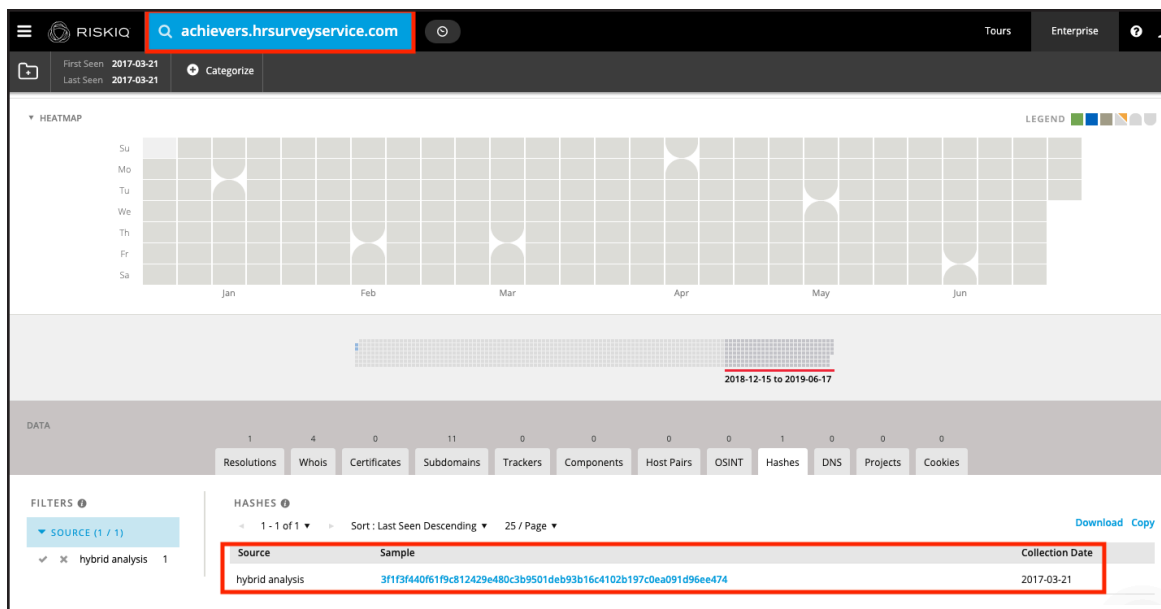
Lucy Template: <https://wiki.lucysecurity.com/lib/exe/fetch.php?cache=&media=prev2.png>

Lucy OEM Edition: <http://lucysecurity.com/wp-content/uploads/2019/03/OEM-edition.pdf>

Additional analysis of this infrastructure associated with the actor groups 2017 campaign and phishing URL surfaced from Hybrid Analysis also show the use of a second Lucy 60 Second Survey template:

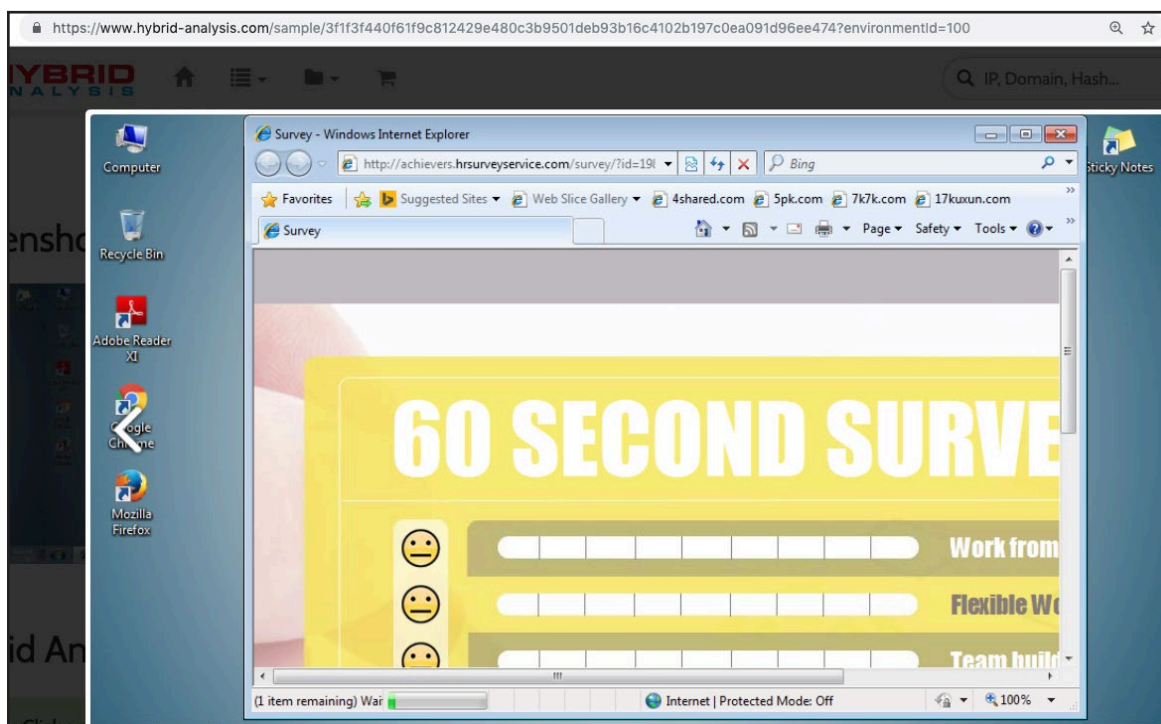
Lucy 60 Second Survey Template

The Lucy platform survey template was used in conjunction with infrastructure hrsurveysservice[.]com and found on a typo squatting host associated with Achievers corp, an employee recognition and rewards platform acquired by BlackHawk Networks.



<https://community.riskiq.com/search/achievers.hrsurveyservice.com>

Analysis of the hybrid analysis match, shows a SendGrid URL scanned using the platform, which redirects to phishing domain achievers[.]hrsurveyservice[.]com, which is using the Lucy 60 second survey template.



<https://www.hybrid-analysis.com/sample/3f1f3f440f61f9c812429e480c3b9501deb93b16c4102b197c0ea091d96ee474?environmentId=100>

With all its automation, Lucy also lets a user easily generate an SSL certificate for its attack campaigns using certificate provider Let's Encrypt, which the attackers did:

The screenshot shows the 'Login & Manage' interface for Lucy. On the left is a sidebar with links: Summary, Scenario Settings, Mail Settings, SSL Settings (highlighted with a red box and a red '1'), Landing Page Template, Message Template, and Errors. The main area is titled 'Scenario Status: Not Started' with a play button. It contains several settings: 'Use Custom SSL Certificate' (checked, with a red '2'), 'SSL Provider' (set to 'Let's Encrypt'), 'Enable Domain Checking' (checked), 'Domain' (set to 'office365.cloudspace365.solutions' with a green checkmark and a red '3'), and 'E-mail' (empty field with a red '4'). A 'Save' button is at the bottom.

Lucy SSL Configuration: https://wiki.lucysecurity.com/doku.php?id=ssl_configuration

Digital Marketing for Phishing Delivery, Tracking, & Analytics

RiskIQ has observed the use of digital marketing solutions such as Sociallab, SendGrid, and Campaign Monitor for phishing email link-tracking. Analysis of known actor-owned phishing domains shows possible victims submitting the tracking URLs to sites such as VirusTotal, Hybrid Analysis, and urlscan.io to determine if the URLs in question are malicious.

The screenshot shows a VirusTotal analysis of a URL. The top section states 'No engines detected this URL'. Below this, a table lists details: URL (http://tracking.sociallab.com/tracking/click?d=...), Host (tracking.sociallab.com), Downloaded file (62461ceba73fa217c92844e3c744e2b982f8c5a4a518d0cef16dccf34f4be33a), and Last analysis (2019-02-04 14:13:57 UTC). A red box highlights the URL and Host fields, with a red arrow pointing to it from the text 'Sociallab Tracking URL'. Below the table, there are tabs for 'Detection', 'Details' (selected), and 'Community'. Under the 'Details' tab, the 'HTTP Response' section is expanded, showing a 'Final URL' (https://hr.euronetworldwide.com.secure-message.online/a34fc9f417efef281sa/) highlighted with a red box and a red arrow pointing to it from the text 'Actor Phishing URL'.

<https://www.virustotal.com/#/url/bbd1d2adc42a3101ace36f8034a9c22d0963ee29612bf0959260957a908d01d9/details>

The use of these analytics and marketing services also aid actors in masking the actual malicious link, allowing them to bypass an organization's security controls, which catch or filter these messages at an email gateway and trick even vigilant users into thinking the link is legitimate.

Additionally, the Lucy platform supports API integrations with external mail servers, highlighting in its documentation how easy it is to integrate with SendGrid. The documentation calls out, "in Lucy, you can use a prepaid, external mail server with an excellent reputation as your default communications method [...]. There are a few advantages to this model especially if all other mail methods of mail delivery fail due to SPAM filtering."

Configuration of using a pre-paid, external mail server (via HTTP)

In LUCY you can use a pre-paid, external mail server with an excellent reputation as your default communication method. In this model, we use an API to Sendgrid (<https://sendgrid.com/>) that allows us to communicate via HTTP to an external mail server to initiate the mail delivery. There are few advantages to this model especially if all other methods of mail delivery fail due to SPAM filtering. You can configure LUCY to use a pre-paid external mail server in two ways:

1. Generic settings for all campaigns: select the HTTP method within "settings/mail settings". You will then be presented the option to define the mails sender domain or mail sender name. This setting will overwrite the individual setting within a campaign and ensure that all emails in LUCY are send using this method:

The screenshot shows the Lucy web interface. At the top is a navigation bar with links: Lucy, Campaigns, Recipients, Sessions, Settings (active), Support, Status, Account, and Logout. Below the navigation bar is a breadcrumb trail: Home / Mail Settings. The main heading is "Mail Settings". Under this heading, there are two configuration fields: "Delivery Method" with a dropdown menu set to "HTTP Proxy", and "Sender" with a text input field containing "phishing" followed by an "@" symbol and a dropdown menu set to "sendgrid.net". Below these fields is a blue "Save" button.

https://wiki.lucysecurity.com/doku.php?id=mail_delivery_methods_in_lucy

Implants & Tools

The attackers make use of several different tools once they have gained an initial foothold via stolen credentials. In general, they employ a combination of legitimate tools for monitoring, remote access, and lateral movement, as well as a combination of Powershell scripts with Mimikatz to elevate privileges or aid in monitoring and lateral movement.

Legitimate Tools

As mentioned, the attackers make use of legitimate tools as part of the infiltration into internal networks of corporations. Because these tools are legal, it makes them harder to spot, particularly if the targeted organizations also use them. However, if they don't, these tools could become excellent indicators of compromise.

Because these tools are legitimate we won't be providing extensive file IOCs as it depends on the used build for a target, all we can denote is that these legitimate tools are part of the attacker's arsenal.

We are aware of the attacker using the following tools during their internal foothold:

- **ScreenConnect:** This tool gives them remote control over a machine in the form of visual (or command-line based) access.
- **EMCO Remote Installer:** This tool gives them capabilities to deploy any tool they want across the network. This tool does require a certain level of access to the network which one of the later discussed PowerShell implants provides them, by using Mimikatz.

Our visibility on these attackers is strictly external, which means we do not have 100% coverage on the aspects of the threat actors' internal movements. The above list includes the only two tools we are aware they use; the odds are that there are more of these tools.

We'd love to collaborate with those who encountered this adversary during incident response to see if we can broaden our knowledge and profile(s).

The attackers also used small PowerShell scripts to rename the ScreenConnect product name on compromised machines:

```
Function DoNotFindMe {
    Try {
        $Keys=Get-ChildItem HKCR:\Installer -Recurse -ErrorAction Stop | Get-ItemProperty -name ProductName -ErrorAction SilentlyContinue
    }
    Catch {
        New-PSDrive -Name HKCR -PSProvider registry -Root HKEY_CLASSES_ROOT -ErrorAction SilentlyContinue | Out-Null
        $Keys=Get-ChildItem HKCR:\Installer -Recurse | Get-ItemProperty -name ProductName -ErrorAction SilentlyContinue
    }
    Finally {
        foreach ($Key in $Keys) {
            if ($Key.ProductName -like "ScreenConnect*") {
                Write-Host $Key.PSPath
                Rename-ItemProperty -Path $Key.PSPath -Name "ProductName" -NewName "XYZ"
                Write-Host "SomethingIsGood."
            }
        }
    }
}
```

These Powershell scripts were staged from remote servers, one example is: serverresults.com/css/indiapro.ps1.11 (MD5: dd5986339aaf23f2baf8c245923a0f69).

PowerShell

The attackers combined their use of legitimate tools with PowerShell scripts taken from public repositories.

BabySharkPro

One of the tools used by the attackers is for the most part a very large PowerShell script which they use to steal credentials and locally stored certificates. We found multiple different builds of the same tool, they contain the same code:

- 28c806cb8c91ab66987ac1ec88344296
- e2e88d6ea5d5d2a4c7b8039988644043
- f6ea268c7e184f580029aec42f2a98f8
- d6472dcebce348d693e68b90099d9ede

The script contains a lot of PowerShell script, which we discuss below, which the attackers encapsulated in one large function scope called **BabySharkPro**:

```
1 Function BabySharkPro
2 {
```

What is more important about this PowerShell script is what it contains: a custom Mimikatz build. The PowerShell script maps a custom build of Mimikatz in memory and runs the following commands to pull down data:

- `sekurlsa::logonpasswords exit`
This command dumps the current and recently logged in users, including password information and some general account information.
- `crypto::cng crypto::capi "crypto::certificates /export"
"crypto::certificates /export /systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE" exit`
Exports the locally stored certificates to disk

The unique thing about these commands is the custom-compiled Mimikatz build on which the attacker used them. The fact that it was custom-compiled makes it an interesting sample—it does not ever hit the filesystem, as it is executed in memory only.

This custom build of Mimikatz was compiled on Saturday, August 4th, 2018, at 00:05:41, which matches the timelines we have on the attacker's activities. The MD5 for this custom build is: 8aea2ae91cc084731a08aa231e79a430.

The code used in the tool seems to be stitched-together modules taken from the PowerSploit module framework: <https://github.com/PowerShellMafia/PowerSploit>.

Empire: Get-Keystores

Another module we found, which shows the attackers sticking with their preference of PowerShell scripts, is a stripped copy of the PowerShell Empire Get-Keystrokes.ps1 module. The attackers removed the comments and author information from the original file from the Empire project GitHub: https://github.com/EmpireProject/Empire/blob/master/data/module_source/collection/Get-Keystrokes.ps1

MD5 for the modified keylogger is: 502fbbdacada9215ed0d026c70f983e1

Staging of payloads

The attackers made use of both the /js/ and /CSS/ subfolders on the server, but this wasn't the only staging method the attackers used. They also made use of GitHub repositories. An account named "onsmooth" maintained repositories which contained PowerShell scripts similar to the one seen on the serverresults.com server.

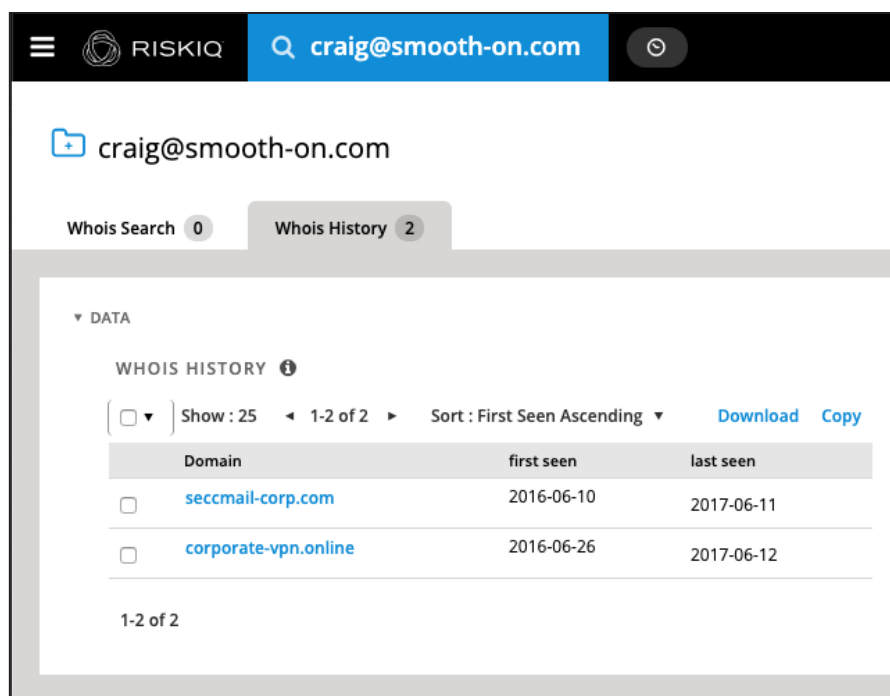


<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
bs.ps1.11	2019-03-12 23:40	6.9M	
indiapro.ps1.11	2019-03-06 20:31	662	
jquery.fancybox-1.3...>	2011-01-13 10:09	8.1K	
reset.css	2011-01-13 10:09	1.0K	
style.css	2011-01-13 10:09	16K	

One example of the used GitHub raw URLs to stage the PowerShell script:

`https://raw.githubusercontent.com/onsmooth/kors/master/bsansi.ps1`

The onsmooth username is also interesting as it mimics a pattern for a domain name used to registered other infrastructure back in their 2016 campaign:



The screenshot shows the RiskIQ interface for a Whois search. The search term is 'craig@smooth-on.com'. The 'Whois History' tab is active, showing a table of domains associated with the email. The table has columns for 'Domain', 'first seen', and 'last seen'. Two domains are listed: 'seccmail-corp.com' and 'corporate-vpn.online', both with first seen dates in June 2016 and last seen dates in June 2017.

Domain	first seen	last seen
seccmail-corp.com	2016-06-10	2017-06-11
corporate-vpn.online	2016-06-26	2017-06-12

Source: <https://community.riskiq.com/search/whois/email/craig@smooth-on.com>

Infrastructure

The infrastructure associated with these attack campaigns highlight how all actors develop patterns and can overlap infrastructure-based operational security failures. This group consistently leverages the same hosting providers, overlaps SSL certificates on common IP addresses, and uses similar WHOIS data which ties infrastructure together.

Hosting Providers

Analysis of the IP addresses used by this actor group show consistent use of the following hosting providers

- Sunnyvision
- Solar Communications
- King Servers

Analysis of the attack infrastructure shows that the actors initially leveraged Sunvision and Solar Communications, two small hosting service providers, to initially host their phishing domains in May and June of 2016 before switching over to King Servers infrastructure in July of 2016.

SSL Certificate Usage and Overlap

Analysis of SSL Certificate data associated with the actors early 2016 IP addresses shows the presence of default Lucy phish platform certificates:

The screenshot shows the RiskIQ interface for the IP address 95.183.52.99. The 'Certificate' tab is selected, displaying details for a certificate issued on 2016-06-09 and expiring on 2026-06-07. The certificate is associated with the domain phish.local. The 'CHANGE HISTORY' section shows a record for 2016-06-13, which is highlighted in orange. The 'DATA' section shows a bar chart with a value of 10 for the 'Certificate' category.

Field	Value
Issued	2016-06-09
Expires	2026-06-07
Serial Number	15377279090054715819
SSL Version	1
Common Name	phish.local (issuer) phish.local (subject)
Alternative Names	
Organization Name	LUCY Phishing GmbH (issuer) LUCY Phishing GmbH (subject)
Organization Unit	LUCY Phishing GmbH (issuer) LUCY Phishing GmbH (subject)
Street Address	
Locality	Thalwil (issuer) Thalwil (subject)
State/Province	Thalwil (issuer) Thalwil (subject)
Country	CH (issuer) CH (subject)

<https://community.riskiq.com/search/95.183.52.99>

The screenshot shows the RiskIQ interface for the IP address 124.248.205.18. The 'Certificate' tab is selected, displaying details for a certificate issued on 2016-06-15 and expiring on 2026-06-13. The certificate is associated with the domain phish.local. The 'CHANGE HISTORY' section shows a record for 2016-06-20, which is highlighted in orange. The 'DATA' section shows a bar chart with a value of 9 for the 'Certificate' category.

Field	Value
Issued	2016-06-15
Expires	2026-06-13
Serial Number	9926094394608921492
SSL Version	1
Common Name	phish.local (issuer) phish.local (subject)
Alternative Names	
Organization Name	LUCY Phishing GmbH (issuer) LUCY Phishing GmbH (subject)
Organization Unit	LUCY Phishing GmbH (issuer) LUCY Phishing GmbH (subject)
Street Address	
Locality	Thalwil (issuer) Thalwil (subject)
State/Province	Thalwil (issuer) Thalwil (subject)
Country	CH (subject) CH (issuer)

<https://community.riskiq.com/search/124.248.205.18>

The presence of these default install certificates from the Lucy platform strengthen the connection to the actors' use of the SaaS security platform as their tool for conducting their phishing attacks against victim targets.

Besides the presence of these default certificates, we were also able to identify common attack infrastructure based on overlaps in self-signed certificates generated and used for the management of the Lucy platform and other infrastructure associated with the actor groups infrastructure, as can be seen in the screenshot below.

The screenshot shows the RiskIQ SSL Certificate Search interface. On the left, there are filters for SHA-1, First Seen, Last Seen, and Unique IP. The main search results table shows one record for the SHA-1 certificate 51d4b4cd19ef174a257840f3d1a419f839014f6d. The detailed view on the right shows the certificate's metadata, including Issued, Expires, Serial Number, and Common Name.

SHA-1	First Seen	Last Seen	Infrastructure
51d4b4cd19ef174a257840f3d1a419f839014f6d	2016-07-11	2016-07-14	185.104.8.160 185.104.8.162 185.104.8.163 185.104.8.164 185.104.8.165 185.104.8.166 185.104.8.167 185.104.8.168 31.148.219.59

<https://community.riskiq.com/search/certificate/sha1/51d4b4cd19ef174a257840f3d1a419f839014f6d>

This certificate overlap and other similar occurrences among this actor group allowed us to surface a significant amount of this actor group's infrastructure across multiple campaigns.

Domain Registrants

While most of the actor-owned domains for this campaign were registered using privacy protection services, RiskIQ analysts were able to identify unique registrant data in historical WHOIS records that assisted us in understanding the broader scope of this attack.

Jacob Rummel

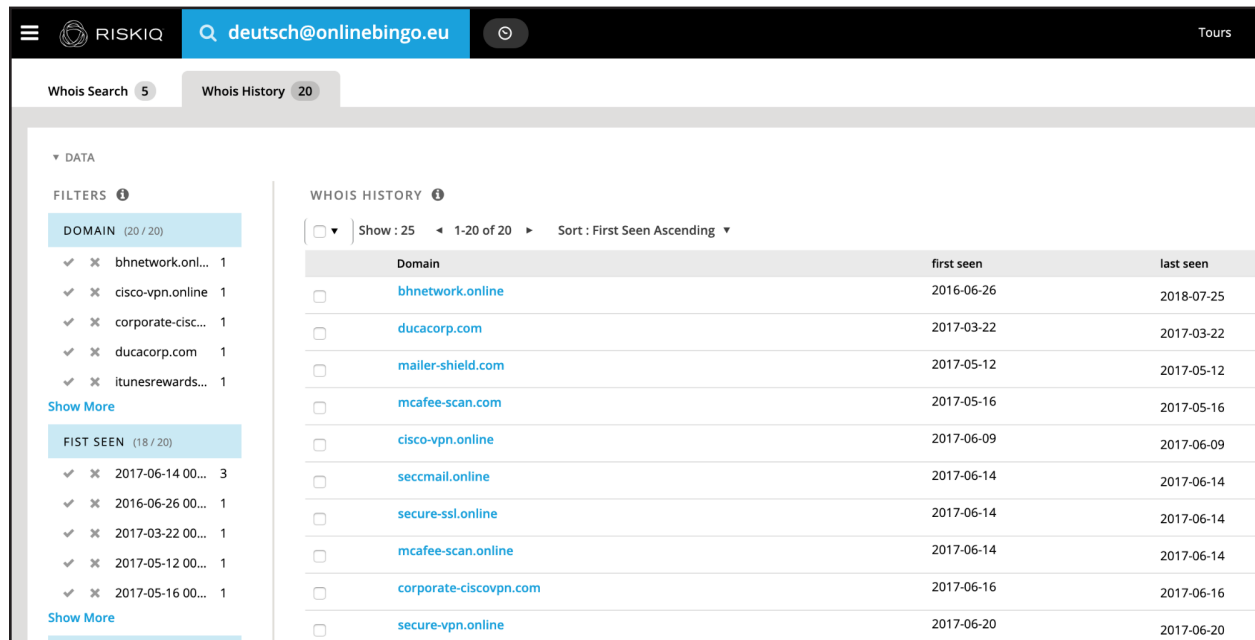
Digging through infrastructure from early 2016's campaign, we were able to surface some early domains registered without privacy protection. As seen in the screen capture below, the domain `bhnetwork.online`, possibly typosquatting Blackhawk networks, one of our actor groups know targets.

The screenshot displays the RiskIQ search interface for the domain `ns1.bhnetwork.online`. The top navigation bar includes the RiskIQ logo and a search bar containing the domain. Below the search bar, a metadata section shows the domain's first and last seen dates (2016-07-05 and 2017-04-22), the registrar (RU-CENTER), and the registrant (Jacob Rummel). A sidebar on the left lists the change history for the domain, with the date 2016-11-23 highlighted in orange. The main panel displays a record from 2016-11-23, which was checked by RiskIQ, expired 2 years ago, and was created 3 years ago. This record contains a table of attributes and values for the domain's WHOIS information.

Attribute	Value
WHOIS Server	whois.nic.ru
Registrar	RU-CENTER
Email	deutsch@onlinebingo.eu (registrant, admin, billing, tech)
Name	Jacob Rummel (registrant, admin, billing, tech)
Organization	Jacob Rummel (registrant, admin, billing, tech)
Street	1078 Avenue Street (registrant, admin, billing, tech)
City	New York (registrant, admin, billing, tech)
State	NY (registrant, admin, billing, tech)
Postal	10023 (registrant, admin, billing, tech)
Country	UNITED STATES (registrant, admin, billing, tech)
Phone	15022932093 (registrant, admin, billing, tech)
NameServers	ns1.bhnetwork.online ns2.bhnetwork.online

<https://community.riskiq.com/search/ns1.bhnetwork.online>

Pivoting off of this unique WHOIS data we were able to surface 19 additional domains registered using the exact same information inside of RiskIQ's historical WHOIS database:



The screenshot shows the RiskIQ interface with the search term 'deutsch@onlinebingo.eu'. The 'Whois History' tab is active, displaying a table of domains. The table has columns for 'Domain', 'first seen', and 'last seen'. The domains listed are:

Domain	first seen	last seen
bhnetwork.online	2016-06-26	2018-07-25
ducacorp.com	2017-03-22	2017-03-22
mailer-shield.com	2017-05-12	2017-05-12
mcafee-scan.com	2017-05-16	2017-05-16
cisco-vpn.online	2017-06-09	2017-06-09
seccmail.online	2017-06-14	2017-06-14
secure-ssl.online	2017-06-14	2017-06-14
mcafee-scan.online	2017-06-14	2017-06-14
corporate-ciscovpn.com	2017-06-16	2017-06-16
secure-vpn.online	2017-06-20	2017-06-20

<https://community.riskiq.com/search/whois/email/deutsch@onlinebingo.eu>

Ivan Wilshea

RiskIQ analysts were also able to identify domains associated with the actors' 2017 attack campaigns with unmasked WHOIS records. One interesting note this time was that the domains in question appear to have initially been registered using a privacy protection service during active usage in the 2017 campaign. However, it seems the protection service lapsed, and the registrar exposed the real WHOIS data in May of this year.

RISKIQ

Q

imail-ssl.com

First Seen 2017-01-22

Last Seen 2019-04-21

Registrar Regional Network In...

Registrant Ivan Wilshea

+

Categorize

CHANGE HISTORY

2019-05-06

2017-11-24

2017-11-22

2017-02-08

2017-01-22

RECORD FROM 2019-05-06

Checked by RiskIQ | Expired 4 months ago | Created 2 years ago

Attribute	Value
WHOIS Server	whois.nic.ru
Registrar	Regional Network Information Center, JSC dba RU-CENTER
Email	yaqhxrccr@emltmp.com (registrant, admin, tech)
Name	Ivan Wilshea (registrant, admin, tech)
Organization	Ivan Wilshea (registrant, admin, tech)
Street	65 W 54th St (registrant, admin, tech)
City	new york (registrant, admin, tech)
State	new york (registrant, admin, tech)
Postal	10019 (registrant, admin, tech)
Country	united states (registrant, admin, tech)
Phone	12122472703 (registrant, admin, tech)
NameServers	expirepages-kiae-1.nic.ru expirepages-kiae-2.nic.ru

<https://community.riskiq.com/search/imail-ssl.com>

A search of the above Name, Organization, and Email address across RiskIQ's historical WHOIS database shows seven domains registered using the same information. Analysis of these domains identified FQDNs used in attack campaigns or as name servers for attack infrastructure.

yaqhxr@emltmp.com

Whois Search 6 Whois History 7

DATA

FILTERS 1

DOMAIN (7/7)

- ✓ x cert-ssl.com 1
- ✓ x hrsurveysevic... 1
- ✓ x imail-ssl.com 1
- ✓ x online-micros... 1
- ✓ x secmail-us.com 1

Show More

FIST SEEN (7/7)

- ✓ x 2018-01-24 08... 1
- ✓ x 2018-01-26 08... 1
- ✓ x 2018-02-16 08... 1

WHOIS HISTORY 1

Show : 25 1-7 of 7 Sort : First Seen Ascending

Domain	first seen	last seen
imail-ssl.com	2018-01-24	2019-04-17
online-microsoft-update.com	2018-01-26	2019-02-26
secmail-us.com	2018-02-16	2019-03-18
xenappvpn.com	2018-02-17	2019-03-19
hrsurveysevic.com	2018-02-17	2019-03-19
cert-ssl.com	2018-03-01	2019-03-02
webex-cloud.net	2018-03-09	2018-03-09

<https://community.riskiq.com/search/whois/email/yaqhxr@emltmp.com>

Conclusion

This analysis highlights how organizations can build off of a small set of network-based IOCs to better derive context about an adversary and their attack campaigns, the scope of their activity, and the overarching impact of the adversary's overall operations. Using a multitude of data sets and pivot points, analysts can gain a broader knowledge of adversary infrastructure

This actor group operated over a sustained period—since at least 2016, targeting specific organization across multiple coordinated campaigns. The use of open-source tooling allowed them to scale their operations while limiting analysts ability to easily attribute activity to a known actor group based on tool reuse. Their operational tempo increased to ramp up targeting and scope over time, which indicates that they achieved at least some success throughout their campaigns

Indicators of Compromise (IOCs)

Due to the size of the infrastructure, the amount of IOCs is much more than what we would put in our report document. We decided to provide appendix documents containing the full set of infrastructure and meta-data around the infrastructure with this report. Please refer to this appendix for the full details regarding the infrastructure.

The [appendix document](#) details are also made available as flat files with this report for quick ingestion.



RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's attack surface. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how the RiskIQ could help protect your attack surface by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net 🌐 RiskIQ.com
☎ 1 888.415.4447 🐦 [@RiskIQ](https://twitter.com/RiskIQ)

Copyright © 2019 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 06_19

The only warranties for RiskIQ products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. RiskIQ shall not be liable for technical or editorial errors or omissions contained herein.