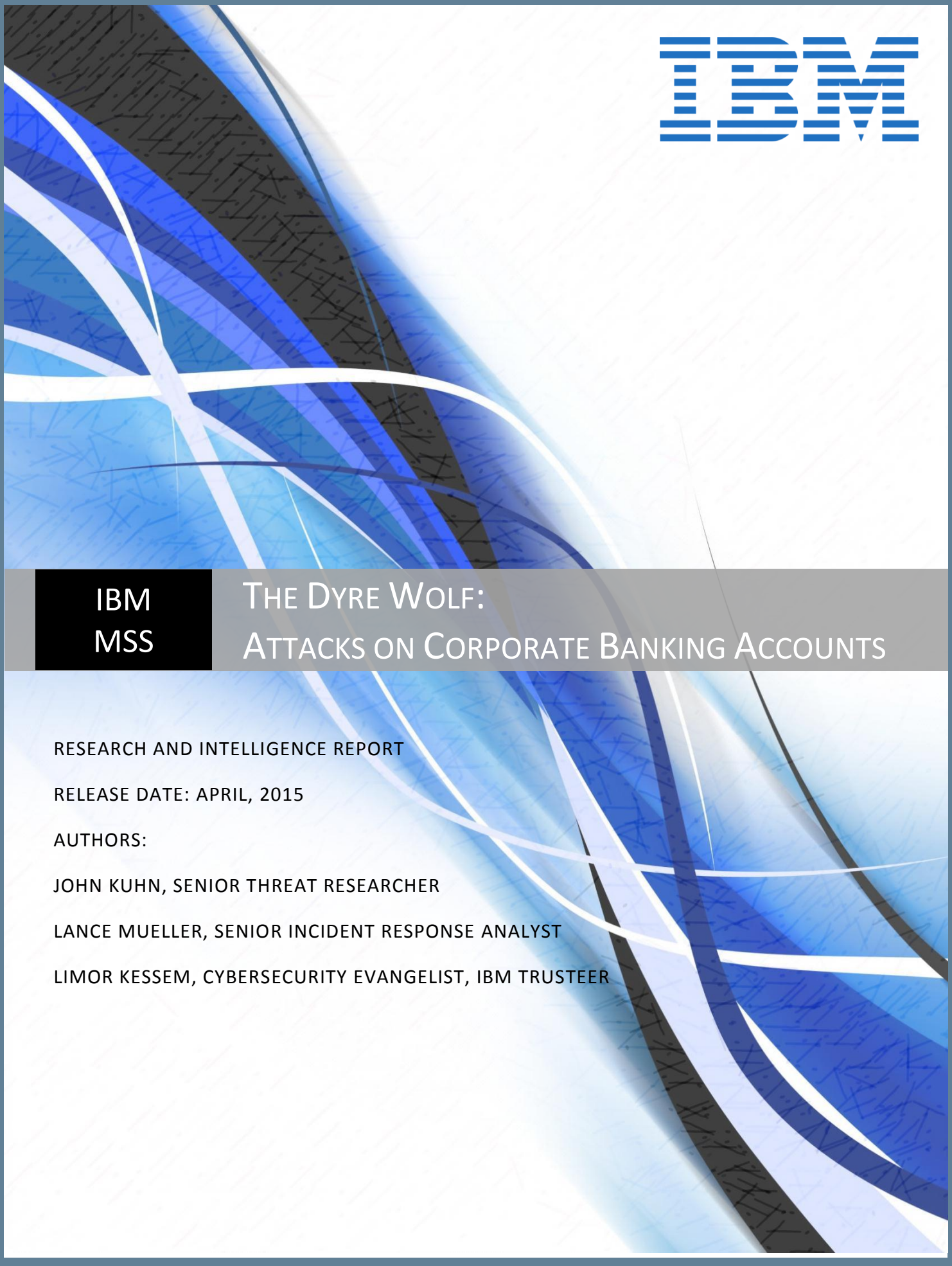


IBM MSS

THE DYRE WOLF: ATTACKS ON CORPORATE BANKING ACCOUNTS

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: APRIL, 2015

AUTHORS:

JOHN KUHN, SENIOR THREAT RESEARCHER

LANCE MUELLER, SENIOR INCIDENT RESPONSE ANALYST

LIMOR KESSEM, CYBERSECURITY EVANGELIST, IBM TRUSTEER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

What do the "Dire Wolf", "Wolf in Sheep's Clothing", and the "Wolf of Wall Street" have in common? Deception, and a ferocious appetite to get what they want. Now, enter “The Dyre Wolf”. This is a new campaign that utilizes the now popular Dyre, or Dyreza, malware directly targeting corporate banking accounts and has successfully stolen upwards of a million dollars from unsuspecting companies. The “Dyre Wolf”, in this case, wants money.

IBM Managed Security Services (MSS) working with Emergency Response Services (ERS) have been tracking a new campaign with a formidable success rate. The organization behind the Dyre malware campaign has not only consistently updated and maintained the malware, they have added more tricks to further their deception. Social engineering via phone calls and denial of service are now part of their toolkit. IBM MSS is tracking several Dyre Wolf incidents across multiple industries and verticals.

Banking trojans, malware designed to leach money from compromised accounts, are nothing new to the world of cyber security. Typically, these targeted accounts are personal checking or saving accounts belonging to individuals that happen to fall prey to the malware. Hundreds, even thousands, of dollars can be transferred out of individual accounts and directly into the attackers’ possession, earning them quick money.

The Dyre malware is one of the most effective banking trojans active in the wild because of its feature-rich capability, and its constant updates which are designed to help it avoid detection by standard security mechanisms. However, while Dyre in itself is rather interesting, it is the group behind this nefarious project that makes a complex campaign so incredibly effective at stealing large sums of money. The infrastructure, the manpower, and the knowledge of banking systems and their websites clearly demonstrate that this group is well-funded, experienced and intelligent.

Spear phishing, malware (initial infection via Upatre), social engineering, complex process injections, the Deep Web and even Distributed Denial of Service (DDoS) sprees are some of the techniques utilized by Dyre Wolf’s perpetrators. However, social engineering and the resulting banking credentials theft is the main focus of this new campaign, and ultimately what's used to directly transfer money from victims’ accounts.

This paper outlines step-by-step how the Dyre Wolf attack is accomplished and outlines techniques organizations can use to detect and prevent compromise.

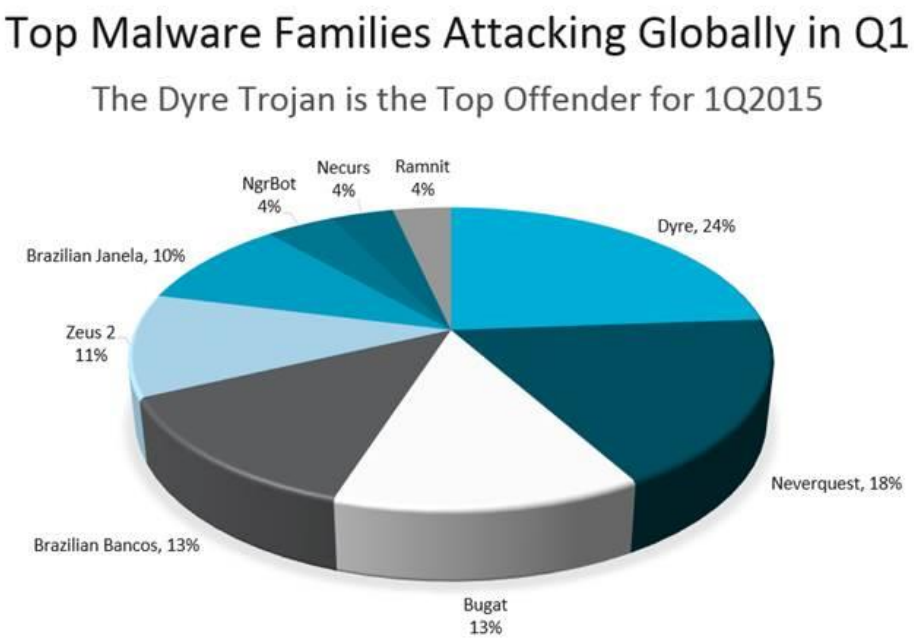
DYRE BY THE NUMBERS

The Dyre/Dyreza trojan started out as a seemingly simple RAT (Remote Access trojan) project around mid-2014. It has since evolved rapidly and aggressively, shape-shifting in both its technical make-up and crime methodologies. At the time of writing this report, Dyre is a full-blown banking trojan that is keeping security professionals guessing, and its victims in remediation mode.

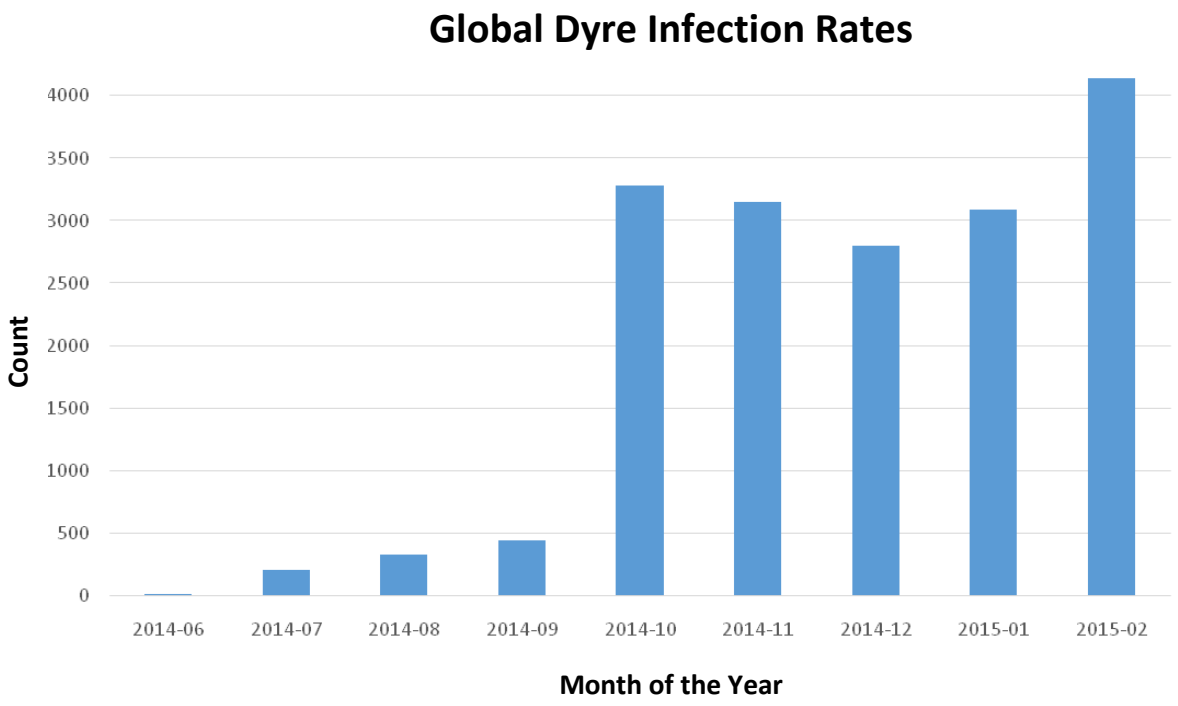
But Dyre, named after a string inside its code that opened "I am Dyreza", was not spawned from thin air. From its early days Dyre had connections to wide bank-targeting spam campaigns, distribution by the Cutwail spam botnet, infiltration via the RIG exploit kit, as well as sharing communication zones with infamous malware like the Feodo trojan, and the Upatre downloader.

According to analysis carried out by IBM Security researchers, an experienced and resource-backed cybercrime gang operates Dyre. It was used in wide-stroke attacks for the past year, and has now moved into a more brazen stage of attacking corporate accounts via the incorporation of skilled social engineering schemes.

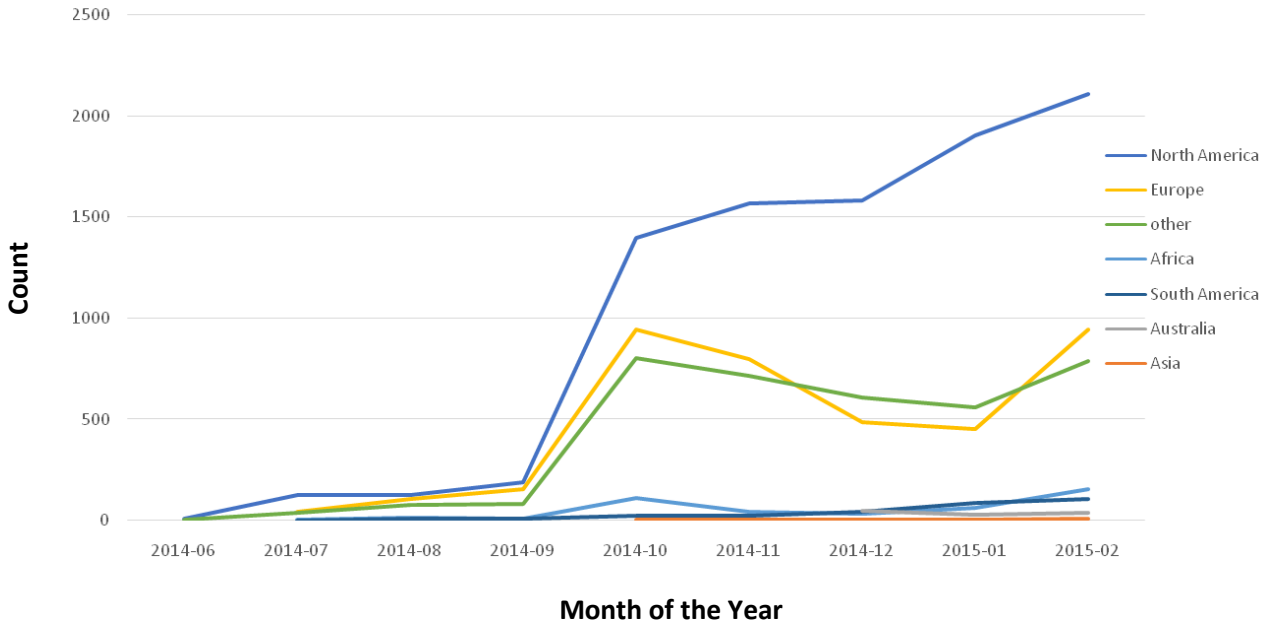
Back in October of 2014, the IBM Trusteer team tracked a very large increase, from 500 instances to almost 3,500, in the infection rate of the Dyre malware. This is now known to be in direct relationship with the development advancements within the Dyre project. In Q1 of 2015, the Dyre trojan was the top offender among the top malware families attacking globally.



From its very early days, Dyre's authors included a mechanism that allows for spreading malware spam through mass mailing of victims' contacts lists. This methodology has always proven effective for malware authors and Dyre takes advantage of it with dramatic results.



North America is the most affected geography seeing highest infection rates of Dyre. This falls in line with the majority of the banks targeted by Dyre's masters.



HOW IT WORKS

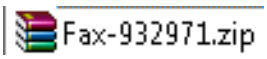
The campaign at hand is a multi-layered attack that is methodical, yet flexible, in order to achieve the goal of high-value financial fraud. Based on evidence collected by IBM Security researchers, the following scenario is the typical methodology used in this campaign and many others like it.

STEP 1: THE SPEAR PHISHING

An employee within the targeted organization receives an email that explains the attached invoice is for their review. It's important to note that this does not have to be emailed directly to their company email. It could also come to their personal account that they happen to check at work.

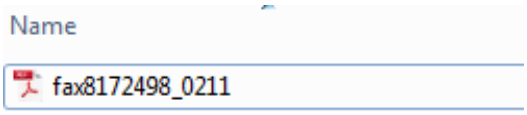
Inside the email is an attached zip file. This file is typically named “invoice*”, “Fax*” or “doc*” with a random number generated behind it.

Example of attachment:

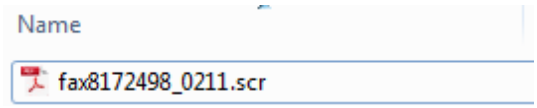


As a second layer of deception, the file inside the zip has an embedded PDF icon, but it is actually an EXE or SCR file. Anyone not paying very close attention would assume that this was indeed a PDF because visually it appears no different. Adding to this confusion, the default Windows behavior is to hide the extension of known file types, which in this case helps the attackers along.

Default windows behavior would show this visual once unzipped:



Whereas, if the user had changed the Windows Explorer configuration to show file extension of known file types, they would see the revealing truth:



The resulting file is the malware known as Upatre (pronounced like “up a tree”), which begins the initial infection of the target machine.

STEP 2: THE FIRST STAGE MALWARE IS EXECUTED

Once the Upatre malware is executed, its sole purpose is to download Dyre. This is completed in a few stages. It's important to note that this stage of the process is completely dynamic. URLs and payloads are constantly shifting in order to evade detection. The Upatre malware itself constantly evolves and remains obfuscated, allowing it to evade antivirus measures as well.

1) Upatre contacts **checkip.dyndns.org** in order to determine the public IP address of the machine it is on. This website replies with a simple message "Current IP Address: x.x.x.x". The malware uses this information to understand who it has infected.

2) Next, a STUN (Session Traversal Utilities for NAT) server is contacted to determine the public IP address and the type of NAT (Network Address Translation) service it's sitting behind.

3) Internet connectivity is checked to determine if a proxy is being utilized by contacting **google.com**.

4) Upatre makes its initial contact with the Command & Control (C&C) server.

5) Upatre downloads Dyre from a varied list of domains as well as changing filenames. For example, metflex(.)uk(.)com hosted a file named “t_image.jpg”, which is the Dyre malware. After utilizing this domain, it is quickly changed, as is the file name for Dyre, including the renaming of the file extension to pdf and txt. Regardless of the domain and URL, Upatre executes this file and begins the stage 2 infection.

STEP 3: THE SECOND STAGE MALWARE IS EXECUTED

Once Dyre is loaded, Upatre removes itself as everything going forward is the result of the extensive functionality of Dyre itself. The password-stealing function of Dyre is the focus of this campaign, and ultimately what's used to directly transfer the money from the victim’s account. Dyre’s set up, much like Upatre’s, requires a number of steps to remain stealthy which helps it to spread itself to additional victims.

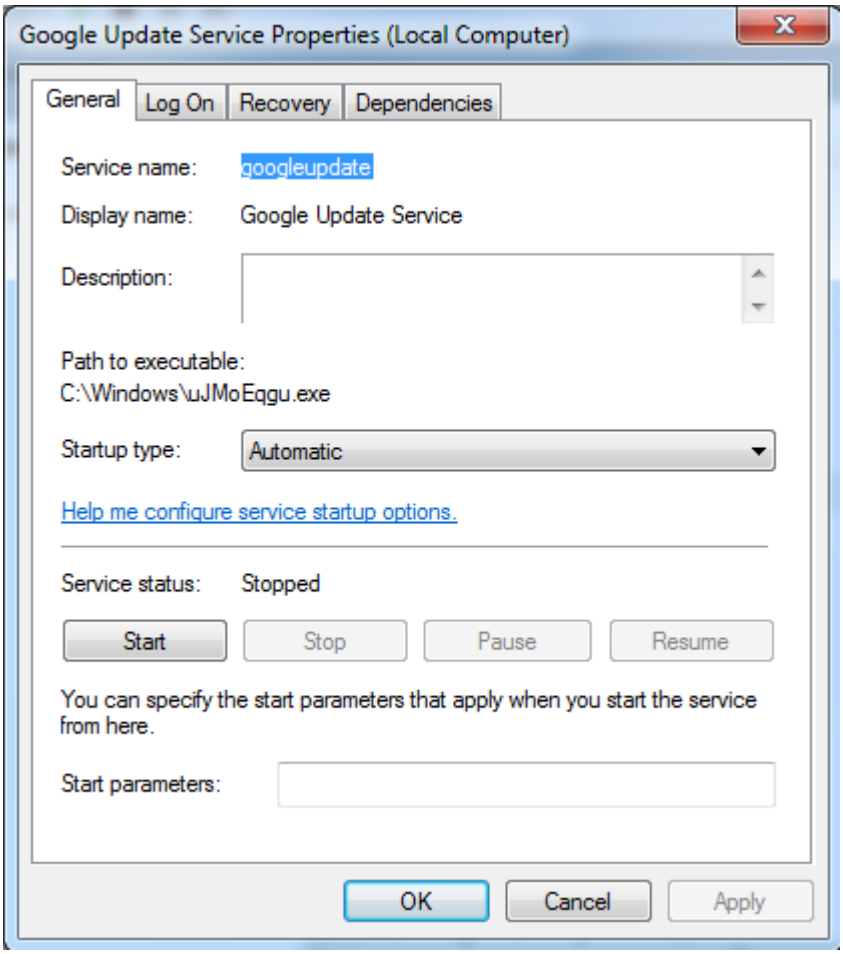
DYRE STAGE 1: ESTABLISHING PERSISTANCE

As part of the installation, the Dyre malware establishes persistence by creating a service innocuously named “Google Update Service”. This service is set to run automatically each time the system restarts.

```
SERVICE_NAME: googleupdate
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\uJMoEqgu.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Google Update Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Once a system is started, it then injects malicious code into the legitimate SVCHOST.EXE process, after which the malicious “Google Update Service” stops.

In the example below, the service was configured by the malware with the startup type “automatic”, but it is currently in a “stopped” state, indicating the injection process has already occurred.



DYRE STAGE 2: ESTABLISHING A DARKNET

During this stage, the Dyre malware makes connections to several I2P (Invisible Internet Project) nodes in order to establish a peer-to-peer tunneling network. This allows information to be sent to endpoint command and control without revealing its final destination or its contents. (For a full list of the used I2P nodes, see Appendix 'A')

The infected system will make several connections to various I2P nodes.

Remote Address	Remote Host Name	Local Port	Remote Port	Process
188.165.213.146	ns371381.ip-188-165-213.eu	49703	4443	636
188.165.213.146	ns371381.ip-188-165-213.eu	49687	4443	636
188.165.213.146	ns371381.ip-188-165-213.eu	49743	4443	636

Note the process ID for the process responsible for the connections is the first instance of SVCHOST.EXE.

Image Name	PID	User Name	CPU	Memory (...	Image Path Name
svchost.exe	636	SYSTEM	00	8,092 K	C:\Windows\System32\svchost.exe

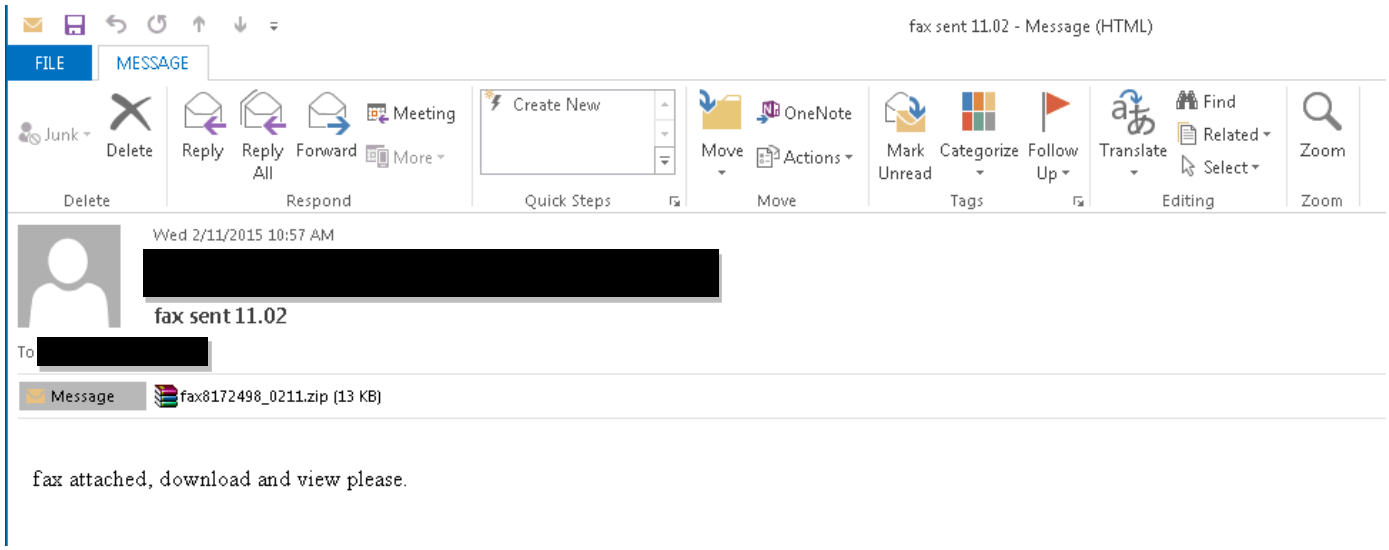
DYRE STAGE 3 – WEB BROWSER HOOKING

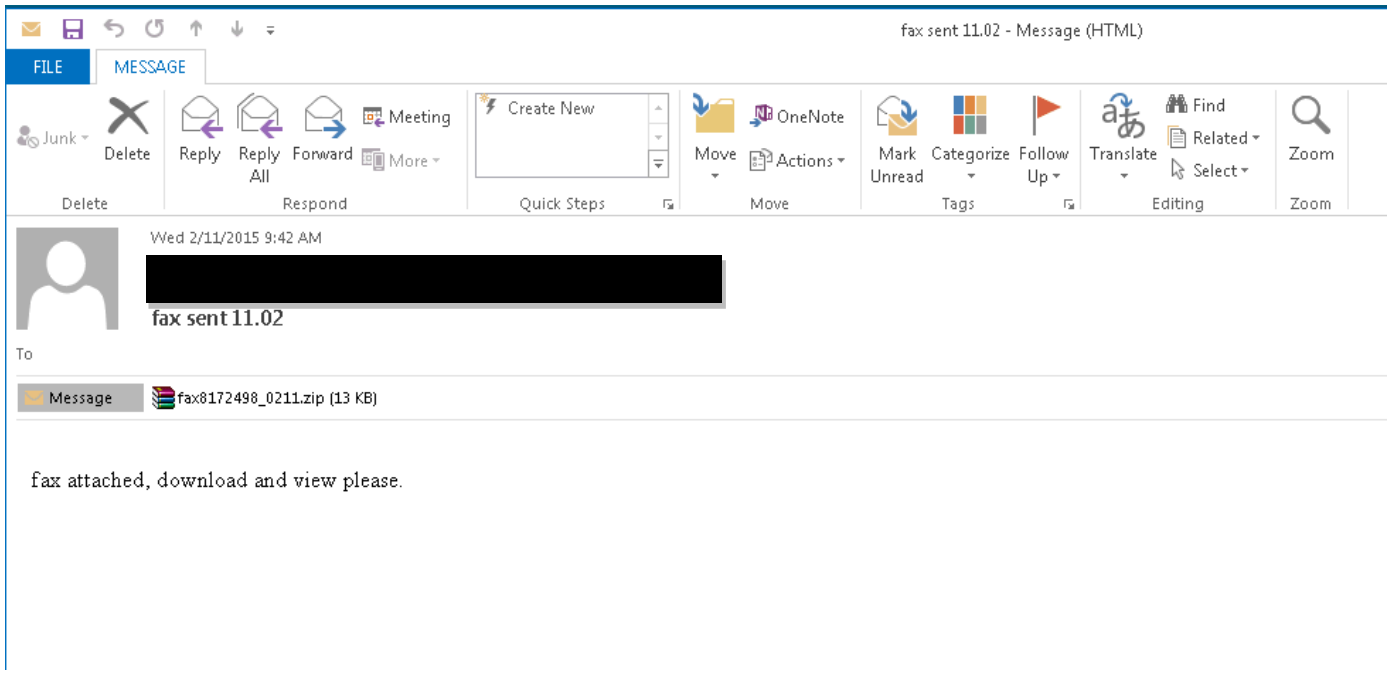
Once Dyre has installed itself and established a solid networking connection, it hooks to the victim's common browsers (Internet Explorer, Chrome & Firefox) in order to intercept credentials the user may enter when visiting any of the targeted bank sites.

DYRE STAGE 4 – EMAIL SPREADING

If Dyre detects that the OUTLOOK email client is installed, it will attempt to send email messages to various recipients with the DYRE payload attached as a zip file. The message content will be fairly vague, but it may be sent to internal and external recipients.

For example these samples are taken from similar Dyre campaigns tracked by IBM X-Force.





These extra emails are being sent by Dyre to infect as many people as possible on its way to growing its botnet and potential victims count.

STEP 4: THE PHONE CALL – ENTER ADVANCED SOCIAL ENGINEERING

Dyre has a number of different ways to operate its social engineering schemes. The MOs vary based on the bank being targeted, but also based on the account the gang is after.

In most cases of attacks on consumer accounts, Dyre uses its elusive technical means to serve the victim with fake messages on screen to lure them into providing personally identifying information (PII) and two-factor authentication (2FA) codes (mostly token generated one-time passwords). Dyre achieves that with three principal flows:

THE CLASSIC INJECTION

In this first flow, Dyre monitors the victim's online activity. The moment the victim attempts to browse to one of Dyre's targeted web pages, the malware injects new fillable data fields into the page, all while collecting the victim's login credentials. This is a classic injection mechanism for banking trojans, it happens on the legitimate original page, and is commonly implemented by malware like ZeuS and all its offspring, SpyEye, GootKit, Bugat, etc.

THE PROXY AND THE WEB FAKES

In a second type of flow, Dyre monitors the victim's online activity. The moment the victim attempts to browse to one of Dyre's targeted web pages, the malware redirects the request through a proxy server over to Dyre's server. In response, the C&C sends back a page replica of the bank's webpage adapted to the original page the victim was supposed to reach. This replica is completely faked and contains extra data fields for the victim to fill out, or messages that will help the attacker swindle money out of the account. These "web fakes" are not part of the bank's genuine website.

ON-THE-FLY, SERVER-SIDE INJECTIONS

In a third injection scenario, Dyre again monitors the victim's online activity. The moment the victim attempts to browse to one of Dyre's targeted web pages, the malware intercepts the response from the bank's servers. It reaches out to its operators' highly secure PHP server, presenting it with the bank's original page response. The PHP server takes over and sends the response to the victim's browser, only this time it includes adapted code injections that are thrown into the bank's response *before* it is served back to the victim. This is an on-the-fly mechanism that Dyre uses to avoid coding its injections into the configuration file. It also allows the attacker to communicate with victims in real time, presenting them with carefully selected social engineering designed to complete a fraudulent transaction.

Considering Dyre's social engineering capabilities makes the next part easier to understand. Reserved for its most high-value targets, Dyre, which has been able to infect enterprise endpoints and take over their bank accounts, puts its best effort into the following scenario.

Here too, Dyre begins by monitoring the victim's browser activity. Once the victim attempts to log into their corporate account on their bank's website, they are presented with an error notice on the banks website that invites them to call the bank about accessing their account (via an injection into the page). The phone number in that message is of course controlled by Dyre Wolf's operators, who are ready and waiting for the victim to fall for it and call.

The victim calls this number and is greeted by a very professional-sounding person with an American accent who states he works with the relevant bank, as if he knew the victim was about to call. After a brief conversation, this

individual prompts the victim to give the username and password in question for the account and verifies it, several times. The attacker may also ask for a token code. Within this verifying stage, the attacker might ask to speak with a co-worker with similar access to the account, and who may be one of the authorized persons on that account, and ask them to verify information as well, and give a token code over the phone.

The attacker assures the victim that the issue will be cleared up soon, and invites them to try accessing the account again in a certain amount of time. While the victim waits for the allotted time to pass the attackers immediately proceed to using the information to transfer a large amount of funds out of the account.

In most cases this step is not needed as the malware itself is capable of recording the credentials and immediately exporting them for use, automating a transaction, or asking for one time passwords in a simple injection. However, it may be that this advanced social engineering step is taken with the intent to defeat more stringent Two Factor Authentication (2FA because the Dyre Wolf operator can ask the victim to read the one time password to them in real time. As long as the criminals log in before the code expires, they will have full access to that account. Many banks also require two people to authorize large money transfers, and this method could further allow the attackers to social engineer their way into obtaining two approval codes on one phone call.

STEP 5: THE WIRE TRANSFER

After obtaining the credentials from the victim, the attacker logs into the account and transfers a large amount of money to various offshore accounts. There have been several reports of compromise resulting in losses of $500,000 to over $1,000,000 USD. This amount of money is staggering and not often seen transferred in one huge sum, as it typically sets off many alerts and becomes incredibly visible to the company and the bank.

It's important to note, these attackers are targeting organizations that typically make large transfers of this size on a regular basis to try to avoid triggering fraud detection mechanisms in place.

Identifying this fraudulent transaction immediately is absolutely critical. The group responsible for the theft quickly moves money from one account to another, making reversal of the transaction often impossible.

STEP 6: THE DDOS

Immediately after the wire transfer happens, the attacker issues a DDoS attack against the victim. The reasons for this are likely several-fold:

1) To distract resources by pulling attention away from identifying and investigating the fraudulent transfer.

2) Hindering or even preventing the victim from logging back into the banking site.

3) Further monetary damage against the victim by impeding them from continuing business online.

The DDoS itself appears to be volumetric in nature. Using reflection attacks with NTP and DNS, the Dyre Wolf operators are able to overwhelm any resource downstream. While they may have the potential to attack any external point in a business's network, the incidents we are tracking appear to focus on the company's website.

WHO IS USING THIS ATTACK?

Dyre, in its current form, appears to be owned and operated by a private and closed cybercrime gang based out of Eastern Europe. The malware code itself could be operated by several teams at once, all of whom are connected to one another and attacking in different geographies.

RECOMMENDATIONS/MITIGATION TECHNIQUES

There are several preventative recommendations that an organization can take in order to stop or limit the risk of the Upatre and Dyre malware.

STRIP EXECUTABLES FROM EMAIL ATTACHMENTS

Most organizations configure their mail servers to prohibit the sending or receiving of emails with executable files as an attachment but will allow zip archives through. This is why it is fairly common for attackers to send an email with a zip archive attachment that contains executable malware. Organizations often configure their email gateways to scan inside of zip archive attachments, but not to strip or remove the executables. If the antivirus scan does not detect the executable as a threat, then it will eventually make it to the user's mailbox and to the endpoint.

When possible, it is recommended that organizations configure their mail server to strip any executable file, including files within archives (that are not password protected) that have an EXE, COM or SCR extension. These files should be stripped before allowing delivery to the user's mailbox.

CURRENT ANTIVIRUS AND/OR ENDPOINT PROTECTION

Endpoint antivirus solutions should never be relied on as the only protection mechanism for threats, but they are the most common initial detection mechanism. It is recommended that organizations ensure their antivirus solutions are updated with the latest virus definitions to maximize their effectiveness. The Upatre and Dyre malware is constantly evolving and changing in an effort to avoid detection. New versions are appearing each day and often go undetected by popular corporate antivirus products for several days.

For example, on March 11, 2015 a new version of Upatre was first seen in the wild and only two out of fifty antivirus products detected it as a threat. The antivirus products commonly used in a corporate environment were not initially detecting it.

File Heuristics:

MD5 : a5c773429e86543747ce8b03314593df
SHA1 : 55065e85ab9723d3b9f8d2b3e2ca0514dae10aae
SHA256 : 8dbbaec774a42e18f369c2bf947a64d03728749b57fad7f46a80ea1ac396af7f
Type : Win32 EXE
First seen : 2015-03-11 15:42:33 UTC
First name : FAX_20150311_1426082680_127.exe
First country: NL
Antivirus products detecting:
ByteHero Virus.Win32.Heur.c
SUPERAntiSpyware trojan.Agent/Gen-Downloader

24 hours later, 29 antivirus products detect it as a threat:

Ad-Aware	Trojan.GenericKD.2214597	**Ikarus**	Win32.Outbreak
Avast	Win32:Malware-gen	**Kaspersky**	Trojan.Win32.Staser.bjef
Avira	TR/Rogue.pwsa.2	**Malwarebytes**	Trojan.Upatre.FD
AVware	Win32.Malware!Drop	**Microsoft**	TrojanDownloader:Win32/Upatre
Baidu-International	Trojan.Win32.Staser.bjef	**MicroWorld-eScan**	Trojan.GenericKD.2214597
BitDefender	Trojan.GenericKD.2214597	**Qihoo-360**	HEUR/QVM19.1.Malware.Gen
ByteHero	Virus.Win32.Heur.c	**Sophos**	Mal/EncPk-ANE
Comodo	TrojWare.Win32.TrojanDownloader.Upatre.A	**SUPERAntiSpyware**	Trojan.Agent/Gen-Downloader
DrWeb	Trojan.Upatre.140	**Symantec**	Downloader.Upatre!gen9
Emsisoft	Trojan-Downloader.Win32.Agent (A)	**TrendMicro**	TROJ_UPATRE.SHMY
ESET-NOD32	a variant of Win32/Kryptik.DBKO	**TrendMicro-HouseCall**	TROJ_UPATRE.SHMY
F-Secure	Trojan.Agent.BIFG	**VIPRE**	Win32.Malware!Drop
Fortinet	W32/Upatre.FT!tr		
GData	Trojan.GenericKD.2214597		

During that 24 hour period, an organization may have received several emails with a malicious attachment that would have gone undetected and exposed the organization to great risk, if executed by end users.

Organizations should consider using different antivirus products for different purposes. For instance, use one antivirus product for the desktops, a different one for servers and another for the email gateway. This strategy can provide maximum coverage with emerging threats that may not be detected by one of the antivirus solutions, but may be detected by another.

In at least one known incident IBM investigated, the antivirus installed on the workstations was not detecting the Upatre malware. However, when the malware attempted to send emails to other users to spread infection, the antivirus product in use on the mail gateway detected the malware and alerted the organization's security team.

Consider the possibility that the initial malware may be received in an employee's personal email account that they check from their corporate device. The employee may directly download the attachment to the local corporate endpoint and it may never be scanned by a corporate email antivirus gateway or otherwise seen by corporate network security tools. In addition to host-based antivirus, organizations can provide another layer of defense against attacks by installing endpoint protection solutions such as Trusteer APEX™ Advanced Malware Protection[1], or endpoint integrity solutions that do not rely on signatures, but rather behavior and trusted applications.

For greater protection, end users are encouraged to download the IBM® Security Trusteer Rapport® software from their bank's website. Protected banks can also be selected from a list on the IBM Security Trusteer website. Since Dyre is financial malware, it is after the bank accounts of users, employees and corporate accounting staff alike. IBM® Security Trusteer Rapport® protects the user's overall online activity and stops malware from tampering with transactions, which ultimately stops fraud in its tracks.

REBOOT AFTER ANY TYPE OF DETECTION

A virus scan may detect and delete or quarantine the Dyre malware that it finds on the file system. But it is important to realize that, because this malware normally only operates in memory as injected malicious code, the malware in memory *will continue to intercept and steal credentials* even after the Dyre files have been detected and deleted from the file system until the system is rebooted.

RESTRICT EXECUTION OF PROGRAMS FROM TEMP FOLDERS

Malware commonly uses temp folders as the initial execution point and Upatre is no different. When possible, it is recommended to use Group Policy Objects (GPO) or Software Restriction Policies (SRP) to restrict the execution of any program from temp folders.

For example, when Upatre is initially executed, it tries to copy itself to the user's temp folder to continue the execution chain. If that were to be blocked, the initial malware infection would be blocked. This is also a common path and behavior for most ransomware and other types of malware.

USE TWO-FACTOR AUTHENTICATION WITH BANKING SITES

While not a fool-proof method of avoiding credential stealing, it is recommended to utilize the maximum security features available from your financial institution's website since corporate bank accounts have such a high

[1] IBM Security Trusteer Apex Advanced Malware Protection: http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware

potential for loss. When possible, enable the use of two-factor authentication at the bank's website for all users who have the ability to login and make transactions. Never disclose your banking portal credentials to *anyone*. A legitimate bank employee will *never* ask for your login credentials or two-factor random number.

Consider using a separate designated host that is specifically configured by the organization for highly sensitive operations such as corporate banking. It should use separate logon credentials, not have the ability to receive company email or freely browse the Internet and should only be allowed to communicate with known trusted or whitelisted destinations.

MAXIMIZE NETWORK VISIBILITY

As with all malware and computer incidents in general, having good visibility across the network is crucial to identifying problems and responding quickly. Since Upatre, Dyre, and other types of malware are constantly evolving, it's unrealistic to try and always know the command and control servers the malware uses and attempt to block them. A better approach is focus on behavior and visibility into the areas that will help you identify anomalies.

In this case, Upatre and Dyre make several fairly static DNS requests to domains such as stun* and checkup.dyndns.org. If your organization does not have a need for these services (STUN or dynamic domains) consider blocking them, but also make sure you have visibility when attempts are made to use them. This provides a real-time alerting mechanism to potential problems that should be investigated further.

This brings up questions that any company should ask themselves:

- Does your organization have the ability to see DNS queries being made across the organization?
- When malicious IPs are identified, does your organization have the ability to route them to a specific sinkhole server that can accept various types of connections for the purpose of 'fingerprinting' the attempted communication?

A typical approach would be to simply block malicious IPs at the egress gateway. However, having a sinkhole system in place provides real-time visibility into devices that may be attempting to visit those sites and provides the benefit of being able to display messages or instructions to end-users explaining why it's blocked or if they need to contact user support.

In several versions of the Upatre malware, the USER AGENT used to fetch the Dyre payload is very unique (Mazilla/5.0 misspelled to trick users it's Mozilla Firefox). This can be used as a trigger to detect some versions of the malware with proper http inspection.

END-USER EDUCATION

Organizations will remain only as strong as their weakest link. Proactive end-user education and security awareness training continue to be critical in helping prevent incidents like the one described in this advisory. It is highly recommended to have periodic training for end-users on the types of threats they are likely to encounter and what actions they should or should not take, especially those users with access to corporate banking credentials. Users should be informed of the common techniques used by attackers, SPAM and phishing campaigns, as well as what actions the organization expects of them if and when they receive unusual emails, phone calls or other communications. Users should know how and who to contact to quickly report anomalies.

Consider doing periodic unannounced mock phishing exercises where the users receive emails or attachments that simulate malicious behavior. Metrics can be captured on how many potential incidents would have happened if it had been real.

INDICATORS OF COMPROMISE

This section contains a list of the STUN servers that Upatre contacts during the initial infection stages and the websites that Dyre waits for the victim to access It's important to remember that Dyre, and campaigns using it, can rapidly change the indicators of compromise. Information contained herein could become obsolete rapidly. However, reviewing your logs historically with this information can be vital in identifying compromises in the past, and today.

STUN SERVERS

In the initial stages of the infection, Upatre contacts one of the following STUN servers:

stun1.voiceeclipse.net
stun.callwithus.com
stun.sipgate.net
stun.ekiga.net
stun.ideasip.com
stun.internetcalls.com
stun.noc.ams-ix.net
stun.phonepower.com
stun.voip.aebc.com
stun.voipbuster.com
stun.voxgratia.org
stun.ipshka.com
stun.faktortel.com.au

stun.iptel.org
stun.voipstunt.com
stunserver.org
203.183.172.196:3478
s1.taraba.net
s2.taraba.net
stun.l.google.com:19302
stun1.l.google.com:19302
stun2.l.google.com:19302
stun3.l.google.com:19302
stun4.l.google.com:19302
stun.schlund.de
stun.rixtelecom.se
stun.voiparound.com
numb.viagenie.ca
stun.stunprotocol.org
stun.2talk.co.nz

COMMAND AND CONTROL

Tracking Dyre via command and control can be a bit of a cat and mouse game. The Dyre malware group is constantly changing their control points as well as masking everything behind the I2P network. This makes it difficult to rely on this single IOC alone, however can be useful to historically review your logs for past indicators.

These command and control hosts were used in incidents involving large money transfers from victims. While they are now outdated, they can be useful to search your logs historically to find infected hosts on your network.

92.240.99.70:12125
92.240.99.70:12124
metflex.uk.com

CONTRIBUTORS

Michelle Alvarez, Senior Threat Researcher

Diana Kelley, Executive Security Advisor

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures suggested by IBM Security Service Teams to remediate the threat. This information is provided "AS IS," and without warranty of any kind.

APPENDIX A: I2P NODES

I2P Nodes Found Hardcoded In Recent DYRE Sample	
46.151.48.114:443	46.63.97.171:443
92.240.99.70:443	46.63.97.224:4443
195.32.89.29:443	46.151.49.53:443
91.210.148.1:443	109.87.231.180:4443
46.151.48.199:443	37.115.203.210:4443
185.31.53.23:443	46.63.97.159:4443
85.94.175.236:443	46.63.97.77:4443
188.165.223.61:4443	46.63.96.198:4443
178.253.216.100:4443	188.165.213.146:4443
188.165.223.61:443	46.63.97.93:4443
91.194.239.109:4443	46.63.96.137:443
46.29.0.247:4443	46.63.97.39:4443
194.28.191.218:443	46.63.96.251:4443
194.28.191.217:443	188.165.213.146:443
176.36.160.107:443	178.212.244.19:4443
46.160.125.167:443	31.131.139.42:4443
91.242.55.58:4443	62.80.181.148:4443
91.225.228.195:443	178.217.49.162:443
77.85.204.113:443	176.119.175.13:443
46.151.50.58:443	176.98.141.2:443
89.22.207.223:443	176.98.133.237:443
188.165.232.226:4443	109.237.0.106:443

I2P Nodes Found Hardcoded In Recent DYRE Sample	
91.202.197.178:443	83.219.158.40:443
31.131.142.226:4443	46.151.48.121:443
195.189.19.156:443	212.36.236.132:443
93.175.224.225:4443	212.36.237.45:443
93.99.229.60:443	212.36.229.141:443
85.248.157.88:443	176.197.103.78:443
188.231.149.4:4443	178.253.251.4:443
194.28.191.70:443	