RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HTA-R04

Dyre Times: Into the Mind of a RAT operator

Note: the deck contains sensitive cyber intelligence findings related to the behavior of cybercrime operators.
No photos please. Censored copy is available upon request.

Uri Rivner
Head of Cyber Strategy
BioCatch
@UriRivner
uri.rivner@biocatch.com

Sam Curry
Chief Technology & Security Officer
Arbor Networks
@samjcurry
scurry@arbor.net

A Dyre Agenda

- Famous RATs: a bit of historic perspective
- Dyre: a security researcher's darling
- Into the mind of a Dyre operator
- Dyre vs. Dridex and other RATs
- RAT trends: Social, Mobile
- Summary

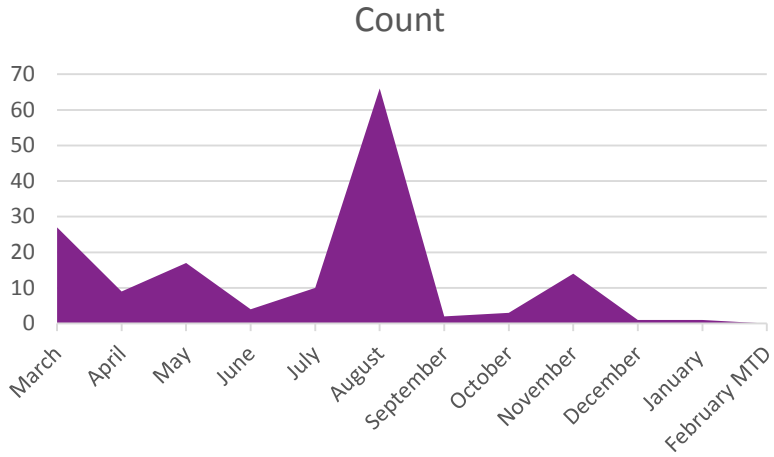
Dyre update!

Latest news

- In November, Russian authorities raided offices of Moscow film company "25th Floor”
- Reuters: 3 sources claimed this was part of Dyre crackdown operation
- Other research orgs corroborating link:
  - Symantec (11/18/15) no new spam campaigns pushing Dyreza were noted
  - Upatre (primary downloader for Dyreza) compromises are significantly down in the wake of the raid:
  - Kaspersky supposedly aided in the takedown
  - There was a presentation about it (Tango with Dyreza) by Peter Kruse of CSIS Security Group

From Arbor

- Mcorral data supports this as well, New Dyreza configs processed



Famous RATs: a *bit* of historic perspective

What are RATs, really?

- Remote Access Trojan? Remote Administration Tool?
  - VNC / RDP / Remote Helpdesk
- Scratch all that – think of a helpdesk taking over your PC scenario
- The benign uses of RATs
- The not so benign uses…

Famous APTs. See anything in common?

Attack	Targets	Malware Used	Going After
Ghostnet 2009	Ministries, Embassies	RAT	Sensitive documents
Aurora 2010	34 companies: Google, Adobe, defense, internet, financial	RAT	Intellectual property
Night Dragon 2011	Critical infrastructure	RAT	Intellectual property
Shady RAT 2011	Dozens of US mega-corporations	RAT	Intellectual property
RSA Attack 2011	RSA (as a security provider)	RAT	Sensitive Security data

Famous Trojans. See anything in common?

A Trojan without RAT is useless

VinnyK
New Member
vXcode
Vendor
Joined: Apr 23, 2015
Messages: 41
Likes Received: 8

http://pwoah7foa6au2pul.onion/listing.php?id=7841
Introducing Kronos, the only actively supported 32/64bit rootkit banking trojan.

Kronos comes with a 64 and 32bit rootkit to provide you with the stealth and compatibility needed for all of your banking operations.

Formgrabber: Kronos has an advanced Formgrabber that doesn't use methods publicly available. It logs ALL POST requests and returns the data to the control panel.

Webinjects: Zeus style webinjects with Kronos style injection techniques. Inject forms and get additional information or automatically transfer funds with the use of Webinjects.

32-bit and 64-bit ring 3 rootkit: Kronos has a very advanced 32 and 64bit rootkit that helps hide and evade user and other bot detection. Great for stealthy operations and helping your botnet live longer.

Proactive Bypass:Kronos uses undetected injection techniques to work without triggering proactice antivirus protection.

Proactive Bypass:Kronos uses undetected injection techniques to work without triggering proactice antivirus protection.

Encrypted Communication: Communication between the bot and the panel is encrypted to help better secure data.

Usermode Sandbox and Rootkit bypass: Kronos can bypass any hook mounted in usermode which allows it to be untouched by other rootkits or sandboxes.

Contact
vinny@exploit.im - please write only with OTR.

https://www.youtube.com/watch?v=IZPzMzK78

VinnyK, Apr 29, 2015

Report Like Reply #8

thelaughingman, s14c14, andgatel and 2 others like this.

SoDumb
New Member
Joined: May 24, 2015
Messages: 4
Likes Received: 0

i dont feel that this should be handled in PM i think we can do it here for other people to see now if i post my proofs that he asked me to send direct etc will you help me get a refund i cannot use it without the VNC so it is essentially useless to me i dont care if it works for other things it simply does not work for my needs which he did not advertise

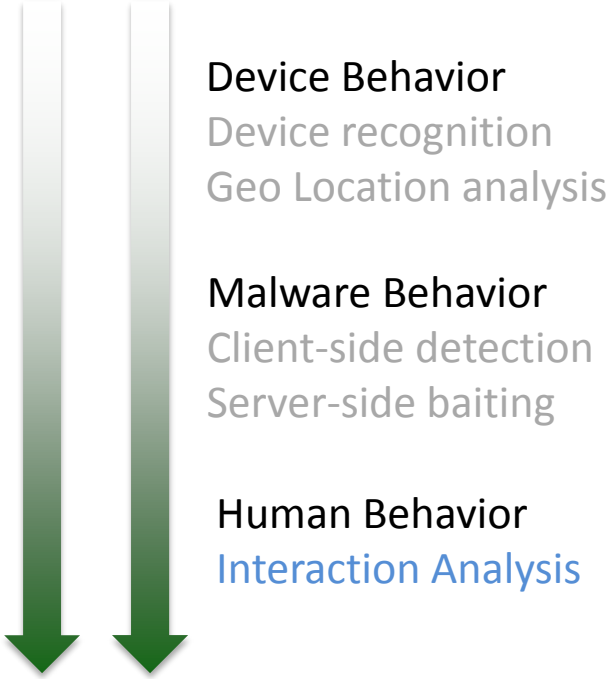
SoDumb, May 24, 2015

Report

help me get a refund i cannot use it without the VNC so it is essentially useless to me

Like Reply #35

Banking Trojans: A New Generation

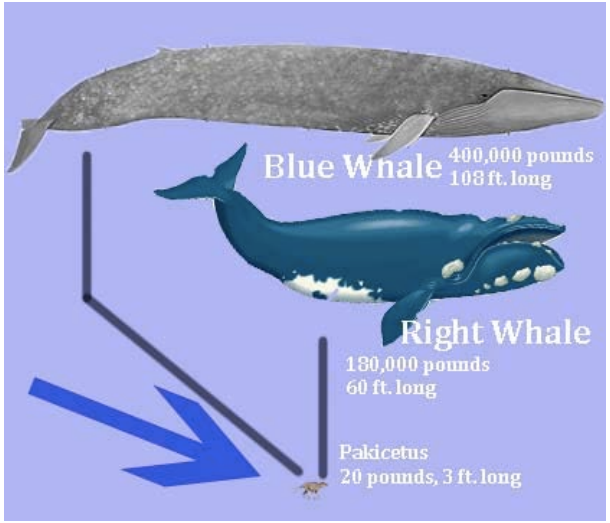


Dyre: the most dangerous Banking Trojan…

… And, just between us –
A security researcher's little darling

General Trends

- Fraudsters are countering security controls in a race to ring 0
- Need to look “normal” means leveraging existing processes and protocols (blend in)
- Divergent evolution of common base anatomy
  - Fraud / Crime: high in the stack, RitB, application land
  - APT / Agenda: whole and low stack
- Adaptive Evolution of Dyre* (incremental, practical improvement)
  - Responding to researchers
  - Selective pressure: profit and effect



A word on naming!

A rose by any other name…

- Infostealer.Dyre
- Variant.Dyreza
- Win32/Dyzap
- Win32/Battdil

Dyre: a (security researcher's) little darling… 1/2

Better C&C

- Dyreza is also more patient about phoning home
- After 7 minutes, successful phone home has usually occurred
- DIF config update and not large batch config update
- Use of I2P hidden servers for C&C – making them robust against discovery and take-down
- Hard coded IPs, (can make some features less adaptive) making sinkholing C&C difficult
- Infostealing config and CnCs hostname/ports found in cleartext

Better Kernel Techniques

- Requires sandboxing the malcode longer - up to 8 minutes
- Sandboxing session terminates before Dyreza phones home
- Lack of CreateRemoteThread() causes sandboxes to lose track
- Sandbox kernel-mode driver thinks all tainted processes have terminated
- Code to prevent running on a single CPU machine
- Uses different technique than NQ for injecting into processes

Dyre: a (security researcher's) little darling… 2/2

Better Local Processes and Tools

- Usually DLL injected into svchost.exe acts as "master"
- DLLs injected into browser(s) acts as "slave"
- Master/slave communications performed via pipes
- Master performs phone homes to CnC to obtain infostealing config

Adaptive analysis needed…

- We hook hook many of theWinInet APIs that Dyreza's master uses to communicate with the C&C,including InternetReadFile, which allows us to intercept the HTTPS commsafter SSL decryption has occurred
- We dump memory of (first) svchost.exe and explorer.exe processes
- We hook NtTerminateProcess() of dropper and suspend it

Dyreza Memdumps (scvhost.exe), 1/2


```
<serverlist>
<server>
<sal>srv_name</sal>
<saddr>46.165.250.138:443</saddr>
</server>
</serverlist>
```

```
<localitems>
<litem>
cashproonline.bankofamerica.com/AuthenticationFrameworkWeb/cpo/login/public
/loginMain.faces*
cashproonline.bankofamerica.com/*
imheskatbeemaopglzsgmp12081.com
srv_name
</litem>
<litem>
businessaccess.citibank.citigroup.com/cbusol/signon.do*
businessaccess.citibank.citigroup.com/*
qcqywynrfgbnyhcjgwelfezdswmk12181.com
srv_name
</litem>
<litem>
www.bankline.natwest.com/CWSLogon/logon.do*
www.bankline.natwest.com/*
xbmagcushtfrlwy12281.com
srv_name
</litem>
<litem>
```

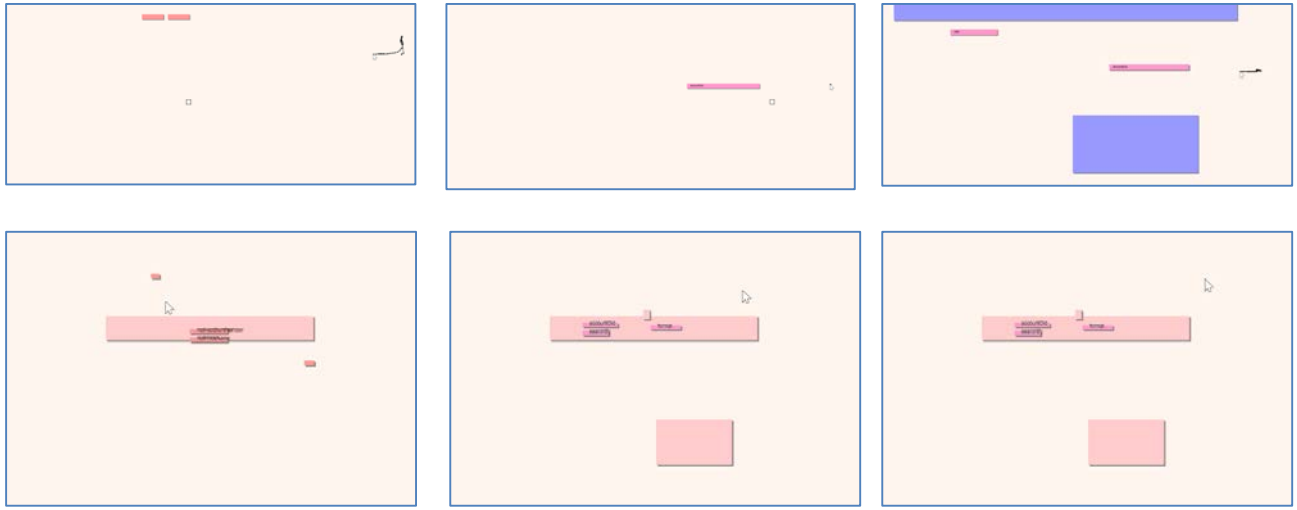
Dyreza Memdumps (scvhost.exe), 2/2


```
<localitems>
<litem>
cashproonline.bankofamerica.com/AuthenticationFrameworkWeb/cpo/login/public/loginMain.
faces*
cashproonline.bankofamerica.com/*
imheskatbeemaopglzsgmp12081.com
srv_name
</litem>
<litem>
businessaccess.citibank.citigroup.com/cbusol/signon.do*
businessaccess.citibank.citigroup.com/*
qcqywynrfgbnyhcjgwelfezdswmk12181.com
srv_name
</litem>
<litem>
www.bankline.natwest.com/CWSLogon/logon.do*
www.bankline.natwest.com/*
xbmagcushtfrlwy12281.com
srv_name
</litem>
<litem>
www.bankline.rbs.com/CWSLogon/logon.do*
www.bankline.rbs.com/*
bnqrcfeeqfn12381.com
srv_name
</litem>
<litem>
www.bankline.ulsterbank.ie/CWSLogon/logon.do*
www.bankline.ulsterbank.ie/*
ogepnfhtubcnqllrz12481.com
srv_name
</litem>
```

Into the mind of a Dyre operator

Behavioral Biometrics: Measuring hand-eye coordination

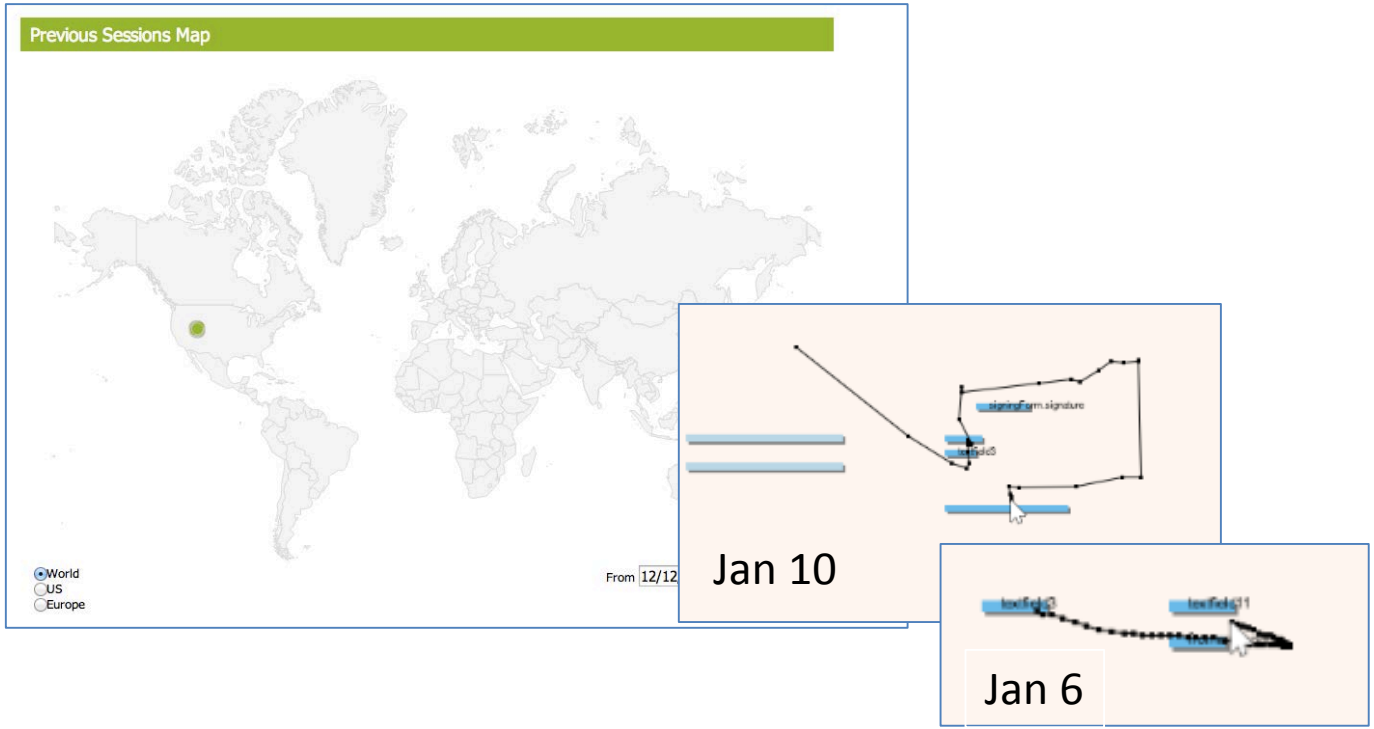
Top: Mouse movement of a user (3 separate sessions)



Bottom: fraudster operating within that user's account

A Mysterious Fraud Case coming from user device

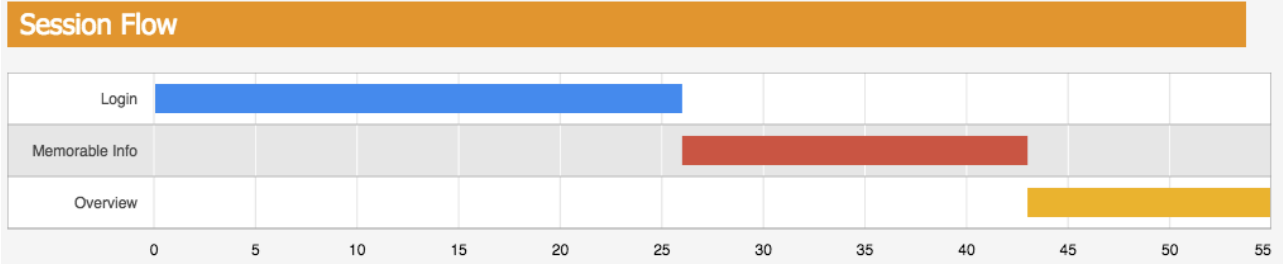
Top 25 US Retail bank



Into the mind of a Dyre Operator

Top 5 UK retail bank

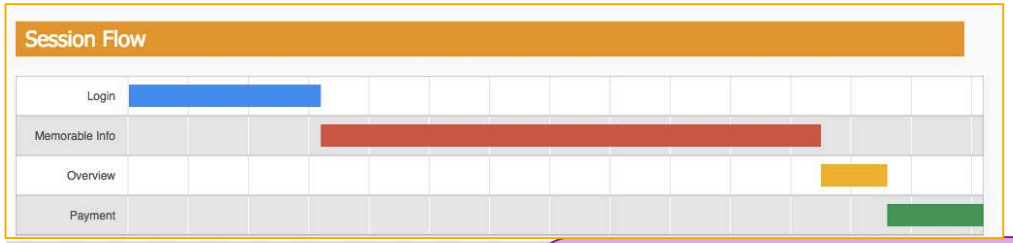
Phase 1: Preparing for the Act



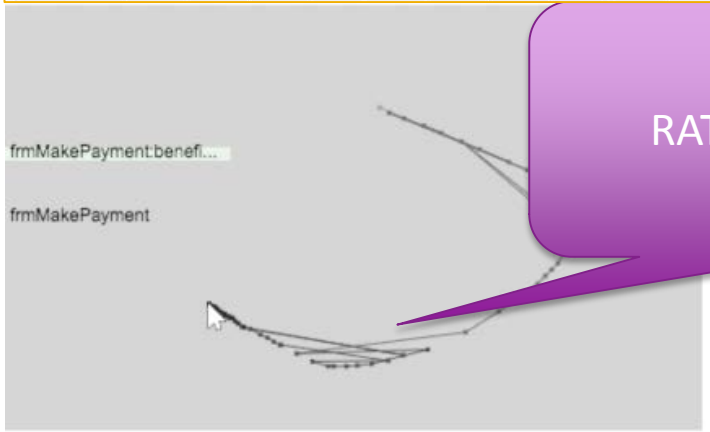
Into the mind of a Dyre Operator

Top 5 UK retail bank

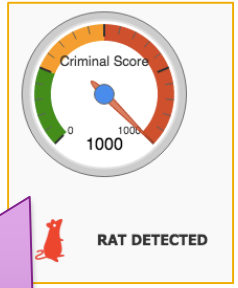
Phase 2: RAT in the Browser attack



2 weeks later – a payment



RAT access using VNC



Detection is possible in two ways: user-focused (user behaves very differently), and threat-focused (RAT signs in the interaction stream)

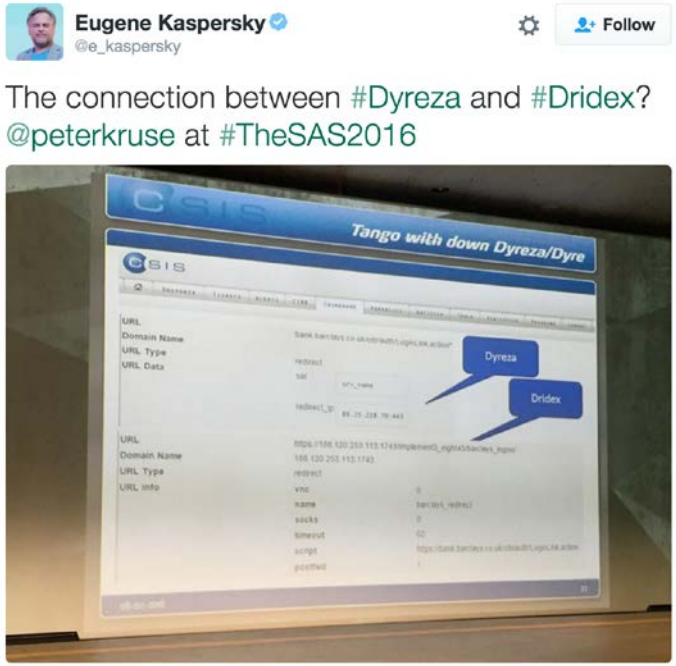
RAT Race: Dyre vs. Dridex and other RATs

Dyre and Dyreza…related?

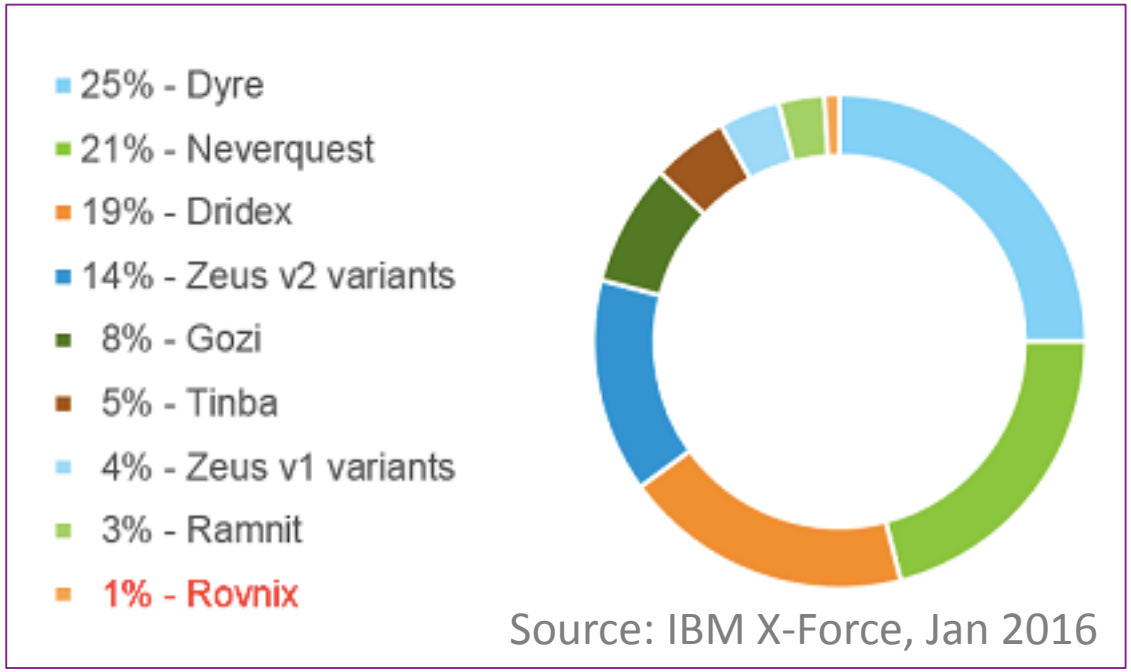
- Dyreza (aka Dyre) is a different malware family to Dridex, although they do have some similarities:
  - Both are banking trojans;
  - Both have been successful as platforms for financial fraud;
  - Both are good at exfiltrating data from the infected hosts;
  - Both appear to be run by well-disciplined, experienced bad guys;
  - Both use encryption for command & control comms;
  - Both are organized into different "campaigns";
  - Both are adaptive and have evolved relatively rapidly;
- Nevertheless, they are not the same malware, nor are they "related" in the sense that one is a descendent/variant of the other.

Or are they…?

- Additionally, we are not aware of any evidence that the operators/authors of the two malware families have any overlap though we don't really spend much, if any, resources on attribution, so we can't be very authoritative about that.*
- This tweet suggests a connection btw Dyreza and Dridex although it is terminated with a question mark…
- Is the slide hinting at a C2 overlap?



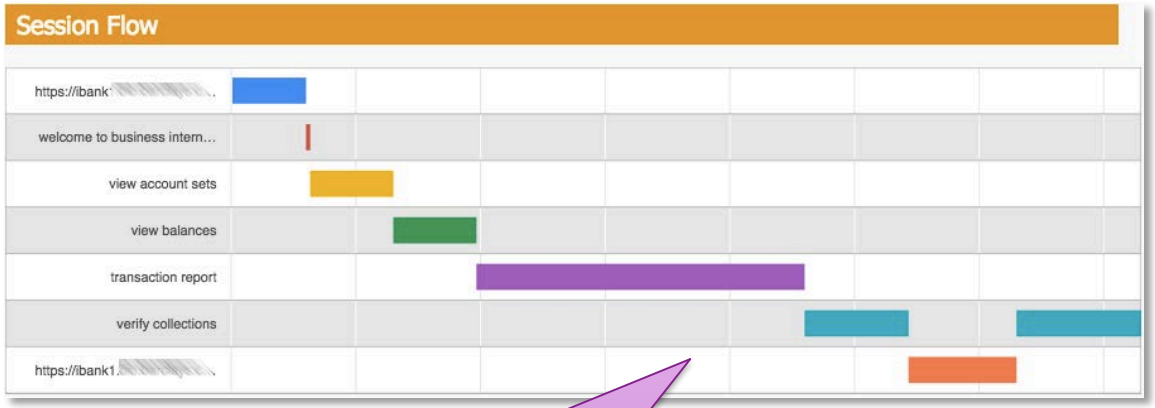
Dyre: #1 Banking Trojan



Source: IBM X-Force, Jan 2016

Dridex

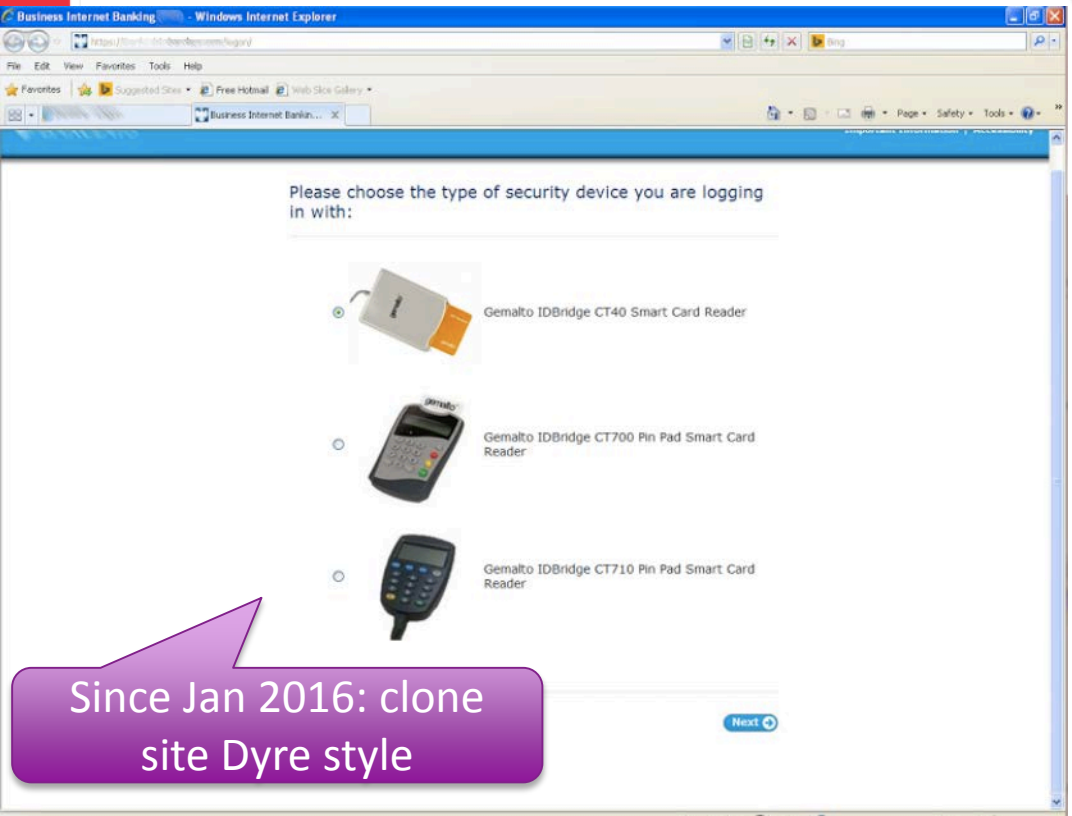
Top 5 UK corporate bank



Regular user

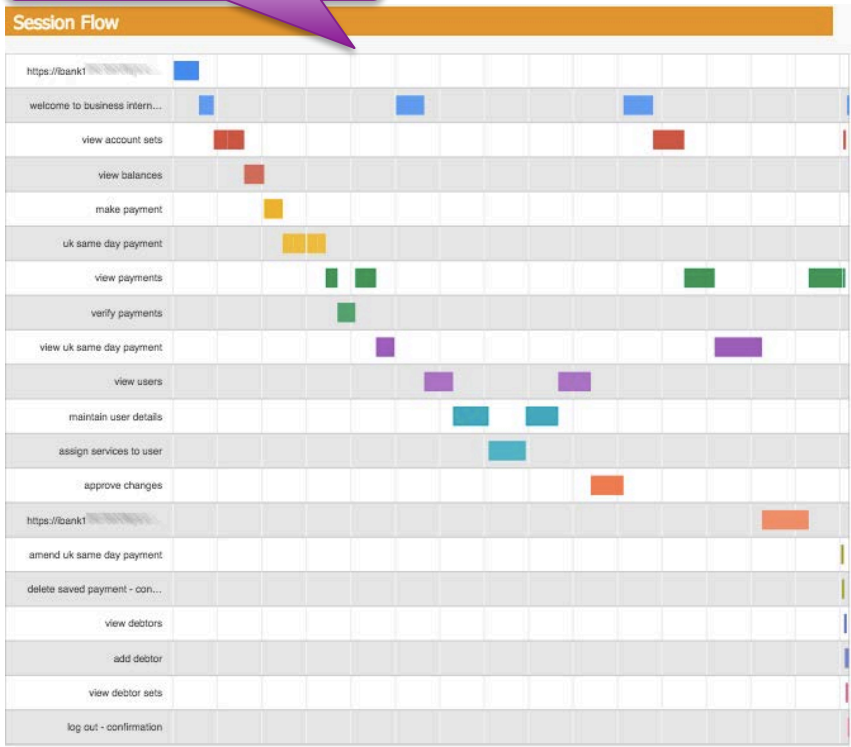
Dridex

Top 5 UK Corporate Bank



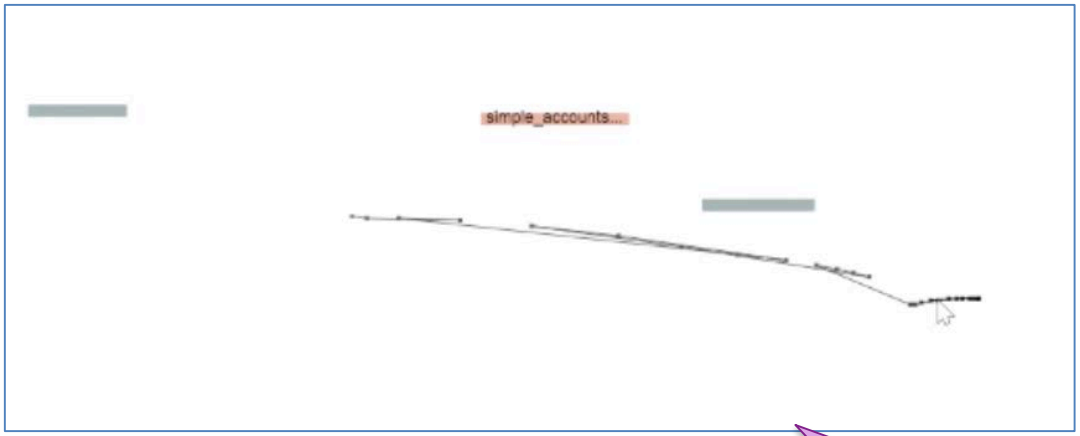
Since Jan 2016: clone site Dyre style

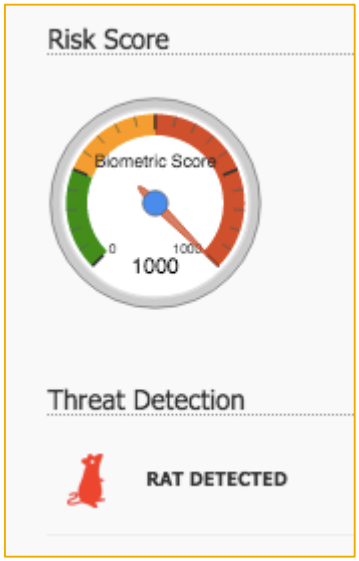
Dridex operator



Dridex

Top 5 UK Corporate Bank



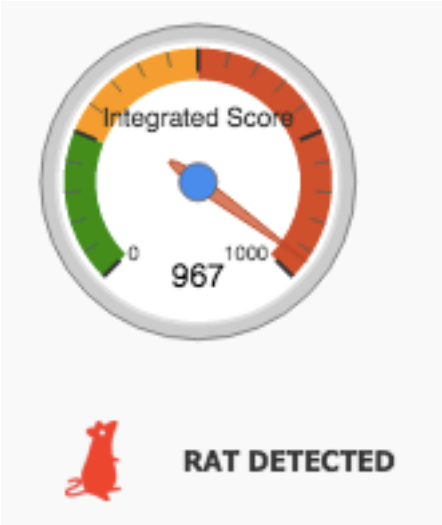


VNC Back Connect

RAT trends: Social, Mobile

The Helpdesk

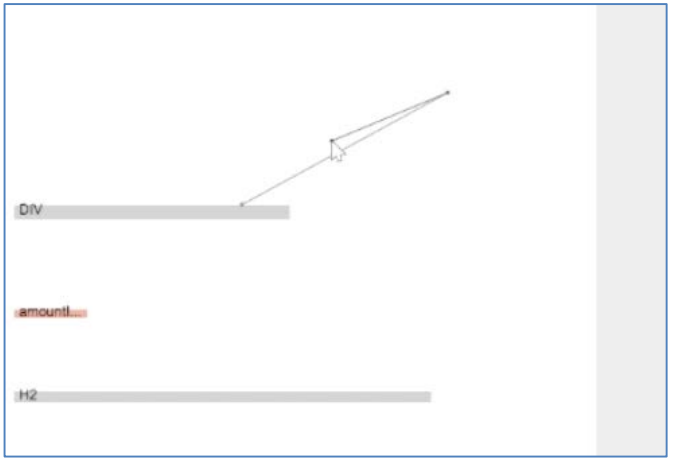
Top 5 UK Wealth Management Bank



The Helpdesk

Top 5 UK Wealth Management Bank

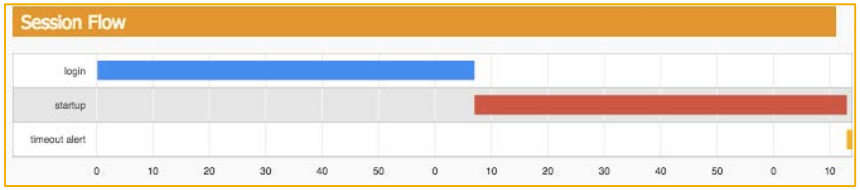
First 2 minutes: legitimate login



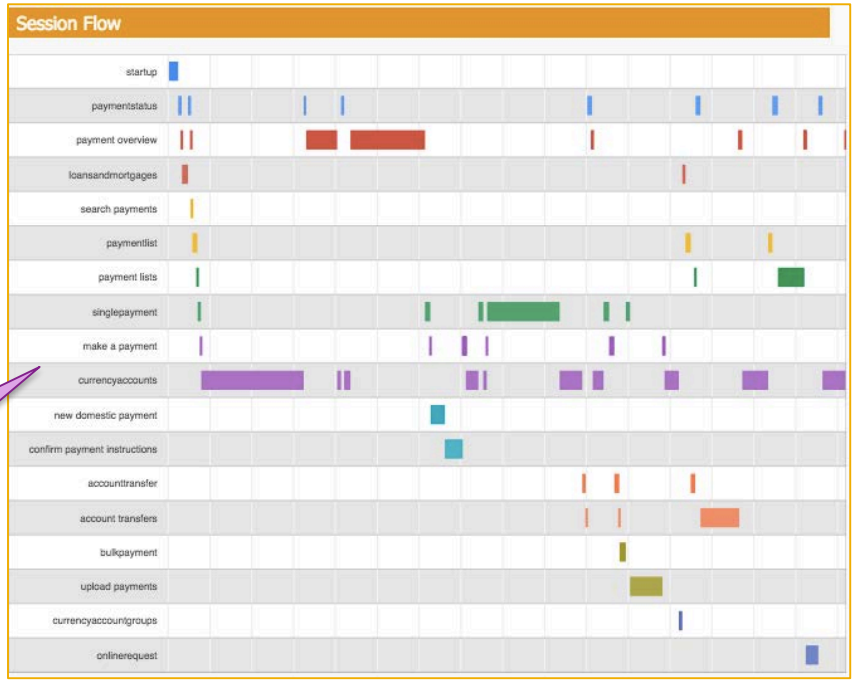
Next 34 minutes: RAT access

New Trend: Social RAT (Team Viewer)

Top 5 UK Wealth Management Bank



Nov 30th Session



Dec 9th Session

Average RAT fraud: $26,000
Average time in account: 31m

When RATs hit your Mobile Device

Summary: Year of the RAT

Apply Slide

Summary

- This is a new-old enemy – don't underestimate it
- Much of the "kit" is 20 years old, the solution is new…treat it as a new threat
- **Dyre**, like Zeus, is a game changer because it neutralizes the contemporary anti-fraud controls and forces the banks to look into a whole new data set to detect it
- **Dridex** is the most dangerous RAT right now
  - The *team* is adaptive and resilient, surviving disruption
  - It heralds what's coming, especially in new media (mobile, IoT)

Next week you should…

- Think about campaigns that target you
- Set up some Google to track NeverQuest, Dyre(za), Dridex
- Consider your mobile security policies vs. the risks. Is it still safe to trust the device?

3 months from today you should…

- Solve the advanced threat problem - j/k ;-)
- Start evaluating different (free, open source and commercial) threat intelligence feeds. Some of the Dyre, Dridex preparatory phase – the social engineering part – is currently detectable
- Look into analyzing user interactions and behaviors. It's a new data domain that can level the field
- Consider long term strategies for winning an adaptive race, especially on new platforms