



SCHOOLBELL AND THE KINGSLAYER

CAN YOU HEAR IT?

RSA[®]

Schoolbell and the Kingslayer

- ▶ About this analyst and team
- ▶ FirstWatch Global
- ▶ What, When, Where, How Much, Why
- ▶ Look into Schoolbell infrastructure
- ▶ A funny domain
- ▶ Suspect Windows event log analysis application
- ▶ A tricky backdoor
- ▶ The Kingslayer attack
- ▶ Lets go back in time
- ▶ Conclusion

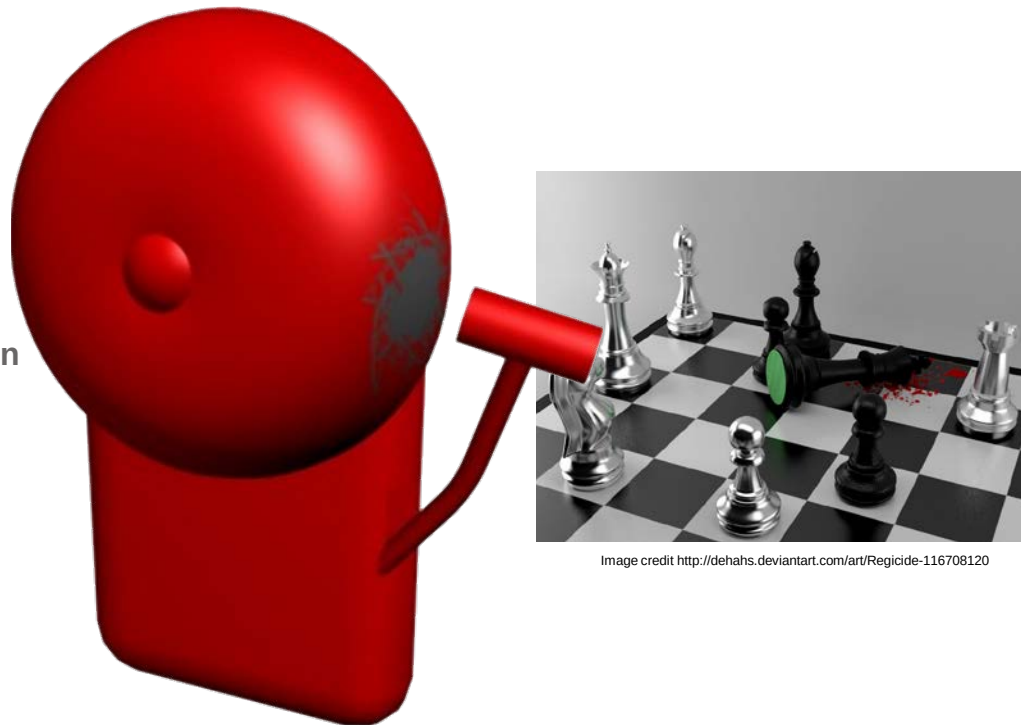


Image credit <http://dehahs.deviantart.com/art/Regicide-116708120>

About the analyst

- ▶ Kent Backman
- ▶ RSA FirstWatch Threat Intelligence Analyst
- ▶ Focus on espionage-related actors
- ▶ Prior: Decade plus all source, intrusion and CIRT threat analysis (sometimes in combat zones)
- ▶ Prior: Oceanography, oceanographic electronics, large-scale web hosting operations, large telescope operations

Project Schoolbell/Kingslayer team

Kent Backman, FirstWatch

Erik Heuser, IR

Jared Myers, IR

Rotem Salinas, FirstWatch

Daniel Frank, FirstWatch

Ahmed Sonbol, FirstWatch

Kevin Stear, FirstWatch

Jon Moroney, FirstWatch

Wes Riley, IR

Christian Roylo, SecureWorks

FirstWatch Global Footprint



A person is sitting at a desk, using a laptop. The laptop screen displays a complex data dashboard with various charts, graphs, and tables. The person's hand is visible, pointing at the screen. The background is slightly blurred, showing a wooden wall and a desk surface.

NEXT

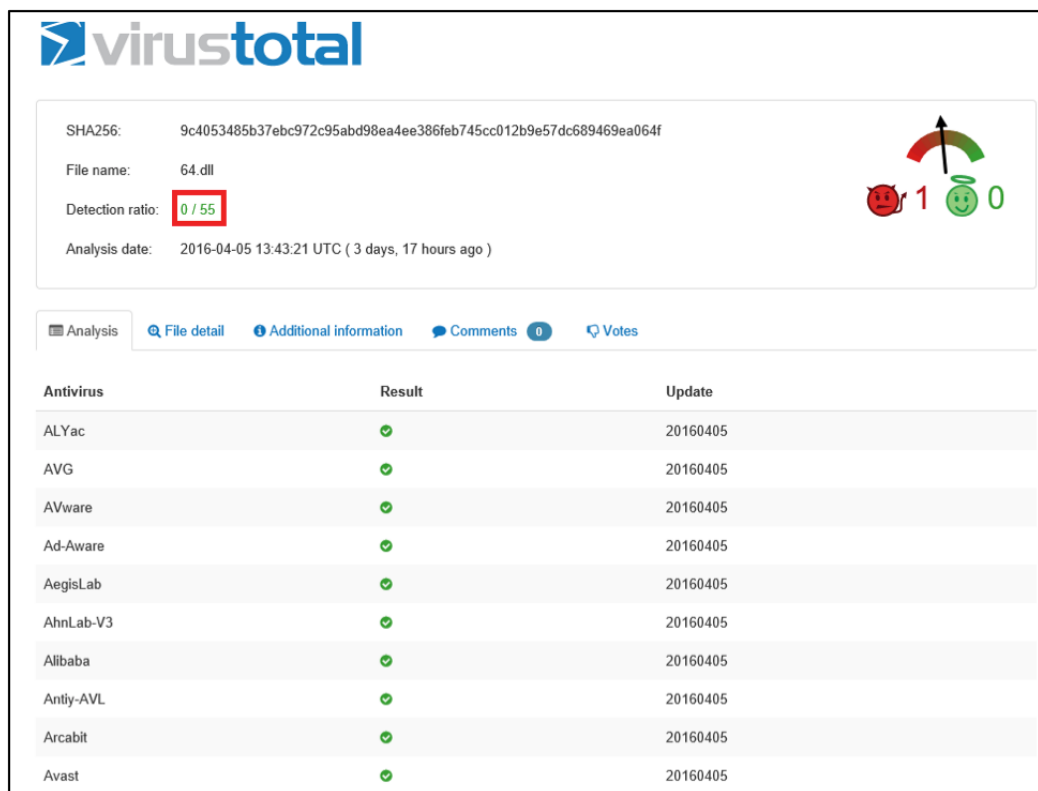
TRY AND FOLLOW ALONG

Schoolbell is a campaign that infected a lot of vulnerable servers

- ▶ **Some people call it a botnet**
 - ▶ old school botnet is a network of zombies, that all have the same C&C, and can respond together to the same instructions (send this spam, attack this site, etc.)
 - ▶ 2k+ systems infected by Schoolbell (that is a way small “botnet”)
 - ▶ six different C2 domains
 - ▶ seven different kinds of malware already described by others
 - ▶ Proofpoint - Exploring Bergard: Old Malware with New Tricks
 - ▶ Palo Alto - New Attacks Linked to C0d0so0 Group
 - ▶ with sometimes multiple variants of each
 - ▶ Harvested by actors more known for their targeted attacks, not collecting botnets
 - ▶ Attribution is not definitive, but these actors appear to fall into the same bucket of malware coding styles, linked infrastructure, and activities named variously as
 - ▶ ShellCrew
 - ▶ C0d0so0/Codoso
 - ▶ APT 19
 - ▶ Axiom

With what were these servers infected?

► Stuff like this

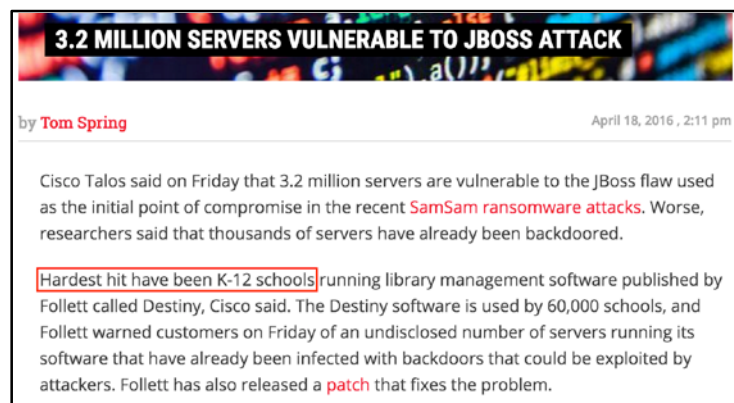


The image shows a VirusTotal analysis page for a file named 64.dll. The SHA256 hash is 9c4053485b37ebc972c95abd98ea4ee386feb745cc012b9e57dc689469ea064f. The detection ratio is 0/55, which is highlighted with a red box. The analysis date is 2016-04-05 13:43:21 UTC (3 days, 17 hours ago). A gauge on the right shows a score of 1 (red) and 0 (green). Below the file information, there are tabs for Analysis, File detail, Additional information, Comments (0), and Votes. A table lists the results of various antivirus engines.

Antivirus	Result	Update
ALYac	✓	20160405
AVG	✓	20160405
AVware	✓	20160405
Ad-Aware	✓	20160405
AegisLab	✓	20160405
AhnLab-V3	✓	20160405
Alibaba	✓	20160405
Antiy-AVL	✓	20160405
Arcabit	✓	20160405
Avast	✓	20160405

How were these servers (most likely) infected?

- ▶ By exploiting vulnerabilities in older versions of JBOSS
- ▶ More recent Java deserialization vulnerabilities affecting other Java web servlet application servers besides JBOSS



3.2 MILLION SERVERS VULNERABLE TO JBOSS ATTACK

by **Tom Spring** April 18, 2016 , 2:11 pm

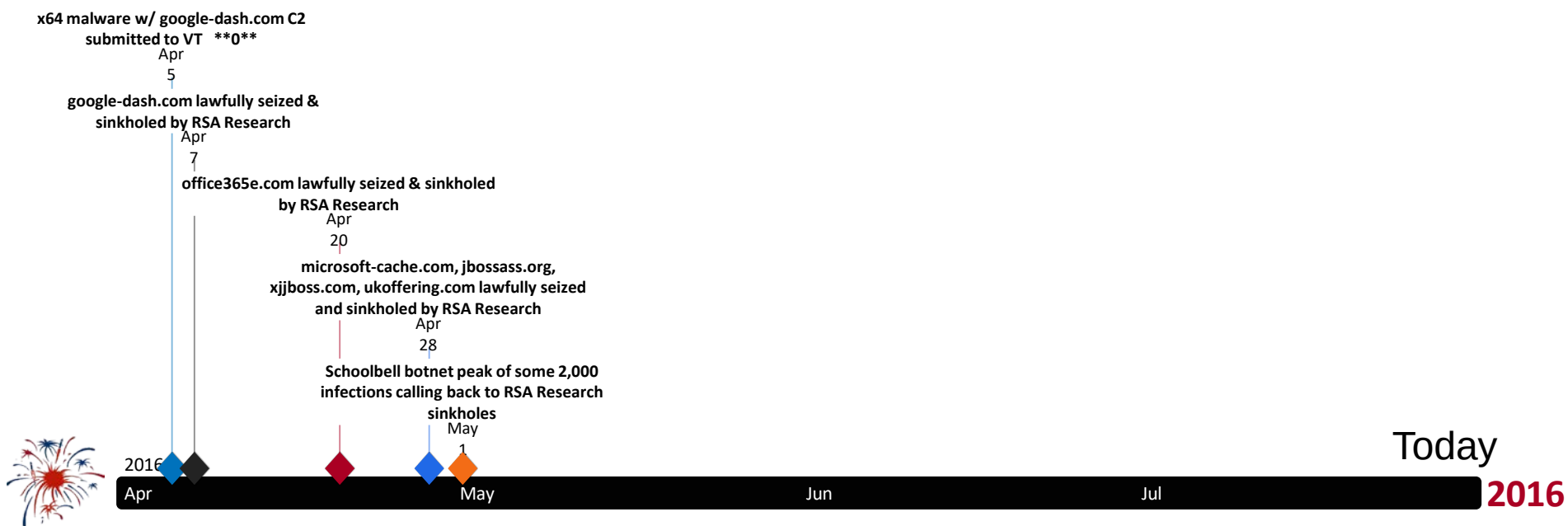
Cisco Talos said on Friday that 3.2 million servers are vulnerable to the JBoss flaw used as the initial point of compromise in the recent **SamSam ransomware attacks**. Worse, researchers said that thousands of servers have already been backdoored.

Hardest hit have been K-12 schools running library management software published by Follett called Destiny, Cisco said. The Destiny software is used by 60,000 schools, and Follett warned customers on Friday of an undisclosed number of servers running its software that have already been infected with backdoors that could be exploited by attackers. Follett has also released a **patch** that fixes the problem.

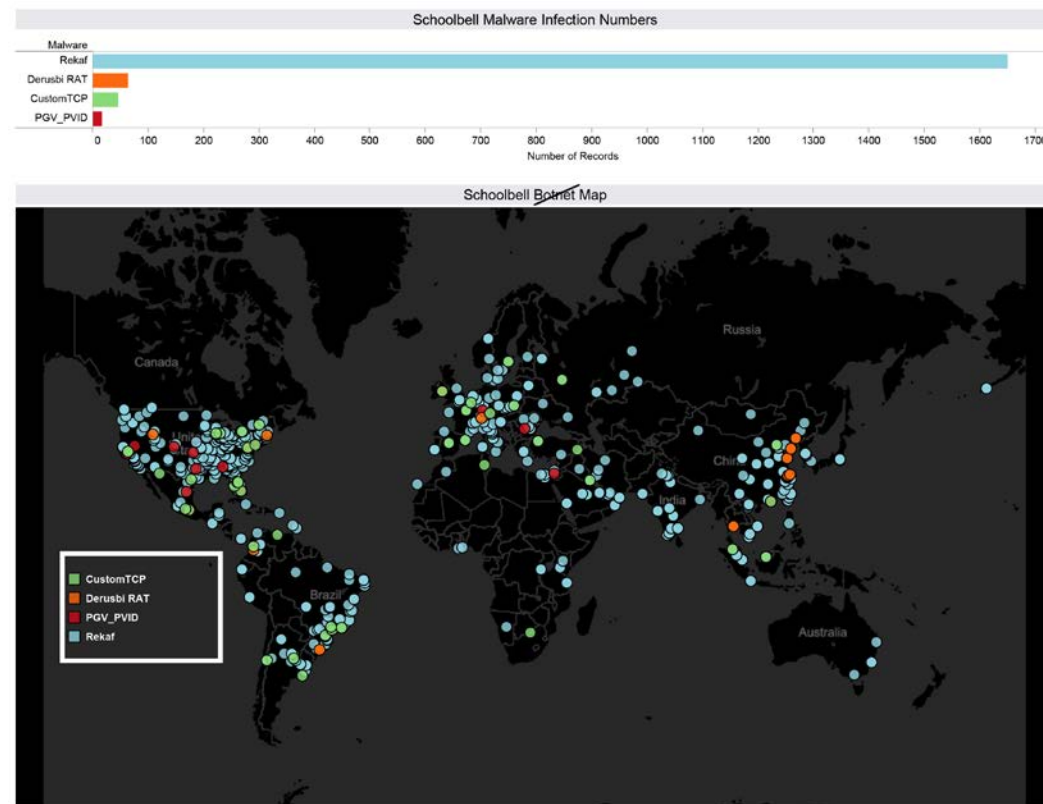
November 6, 2015

What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? This Vulnerability.

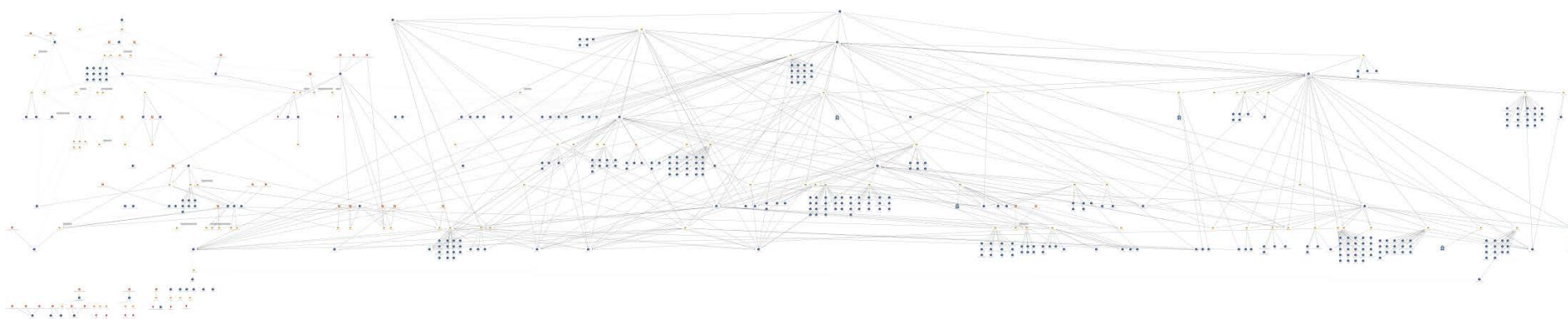
By @breenmachine



Where are these servers that are infected?



A lot of operational actor infrastructure



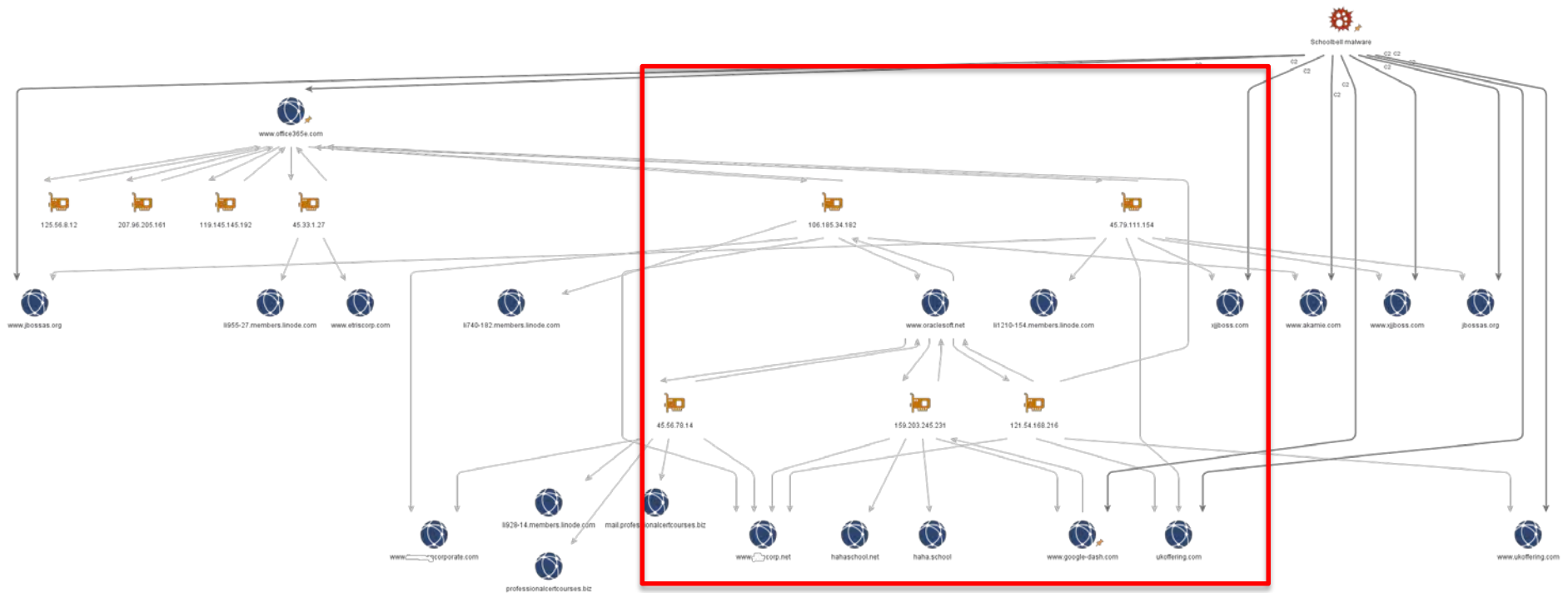
Linked with:

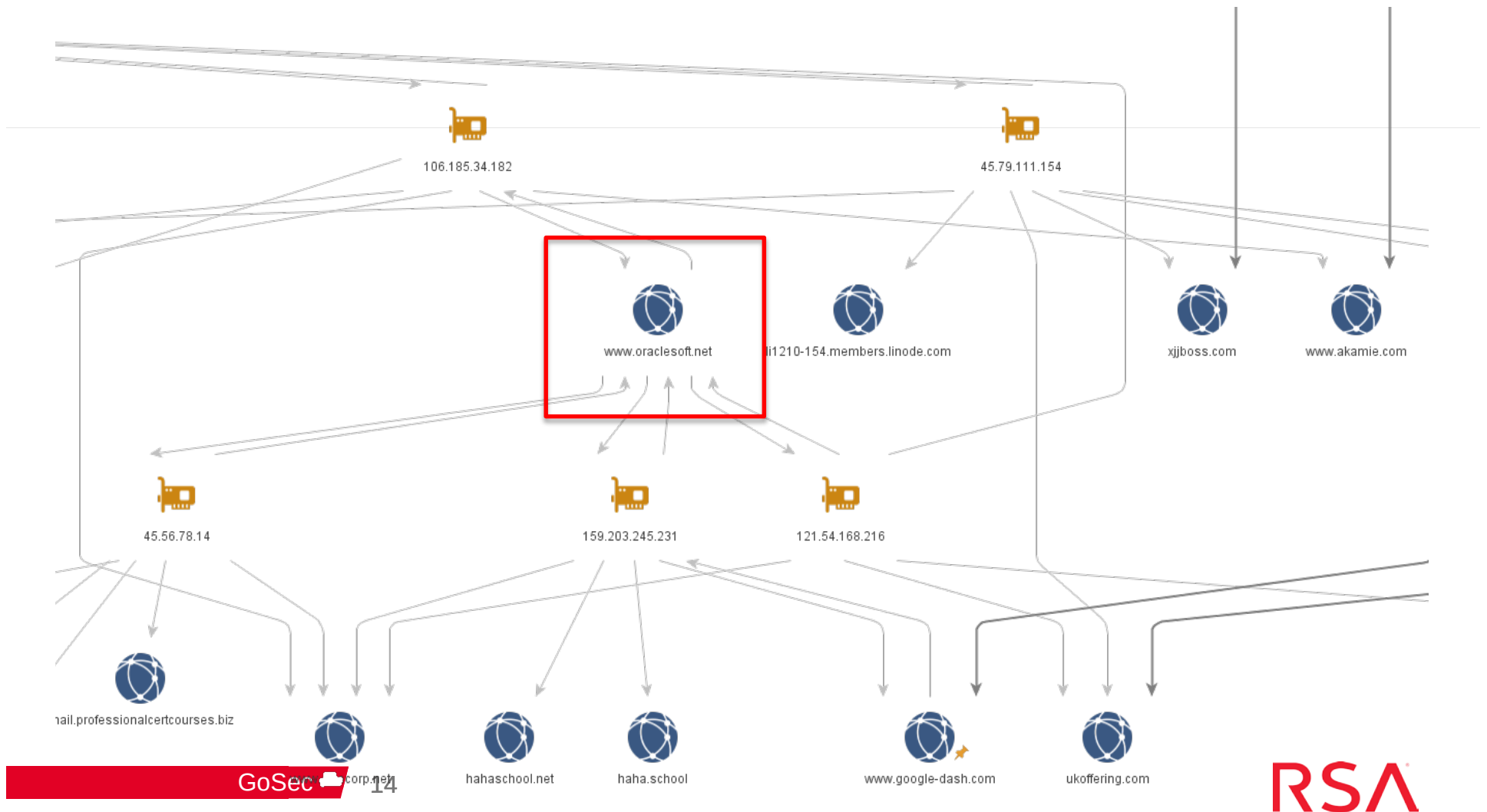
1. Malware clusters
2. C2 domains and IP addresses
3. Historic DNS resolutions (pDNS)

Why did they hack thousands of servers?

- ▶ **Our research partner SecureWorks has observed significant exploitation activity originating from Schoolbell-infected, targeting SecureWorks customers**
 - ▶ Is Schoolbell being used as a hacking launch point by advanced actors?
 - ▶ We don't know: the same vulnerabilities could have given other actors access.
- ▶ **Schoolbell-related Remote Administration Tool (RAT) called TXER was deployed with DDoS plugins**
 - ▶ Every system so far we forensically examined w/ other Schoolbell malware also had TXER
 - ▶ Many code similarities with other Schoolbell malware
 - ▶ Is Schoolbell used for DDoS attacks by advanced threat actor?
 - ▶ If so, it would be the first time we have seen it from these actors
 - ▶ We don't know how many hosts are infected with TXER because it uses Peer to Peer (P2P) communication over an anonymous encrypted protocol called Tox
 - ▶ Difficult to interdict unlike like other Schoolbell malware
 - ▶ RSA Research in Israel continues to analyze TXER

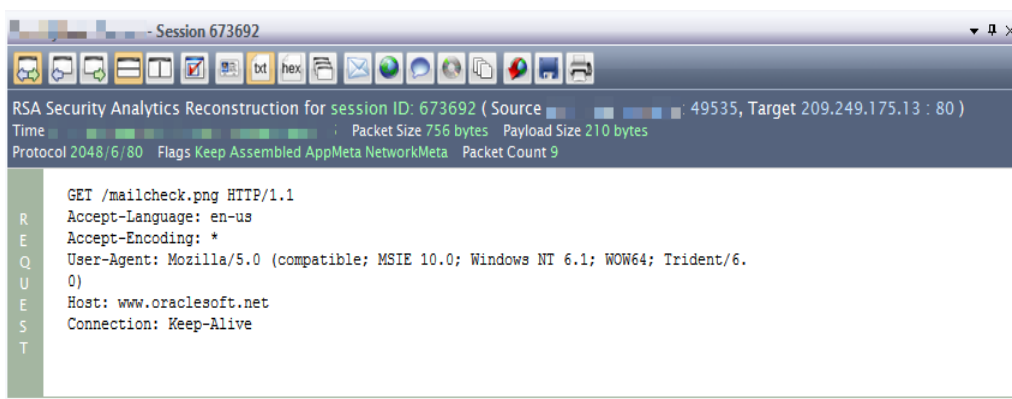
Lets look closer at some Schoolbell infrastructure





(Some sources and methods protected)

- Observed evidence of beaconing to www.oraclesoft.net



The screenshot shows a window titled "Session 673692" with a toolbar containing various icons. Below the toolbar, the text reads: "RSA Security Analytics Reconstruction for session ID: 673692 (Source [redacted] : 49535, Target 209.249.175.13 : 80)". Below this, it says "Time [redacted] Packet Size 756 bytes Payload Size 210 bytes". Further down, it says "Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 9". On the left side, there is a vertical label "REQUEST". The main content area displays the following text:

```
GET /mailcheck.png HTTP/1.1
Accept-Language: en-us
Accept-Encoding: *
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Host: www.oraclesoft.net
Connection: Keep-Alive
```

- Spent considerable time on the phone
- Performed forensic investigation of an unsuspecting organization's Windows domain controller
- Head scratching and discussions
- Reverse engineering (IR Team) of a *suspect Windows event log analysis application*

Now I know why dynamic analysis was tough

```
private DateTime UpdateDateTime()
{
    DateTime dateTime = TimeZoneInfo.ConvertTimeToUtc(DateTime.Now, TimeZoneInfo.Local);
    return TimeZoneInfo.ConvertTimeFromUtc(dateTime, TimeZoneInfo.FindSystemTimeZoneById(Evlog3fu.Decrypt("HCvEV8XntwR2ASf98CqT5Eu-", "EvlogServiceInstaller")));
}
private bool IsData(DateTime pluginDt)
{
    return pluginDt.DayOfWeek == DayOfWeek.Saturday || pluginDt.DayOfWeek == DayOfWeek.Tuesday || pluginDt.DayOfWeek == DayOfWeek.Thursday || pluginDt.DayOfWeek == DayOfWeek.Friday;
}
public void Run()
{
    try
    {
        IL_00:
        while (this._Run)
        {
            DateTime pluginDt = this.UpdateDateTime();
            if (!this.IsData(pluginDt))
            {
                Thread.Sleep(600000);
            }
            else
            {
                while (this.IsData(pluginDt) && pluginDt.Hour < 9)
                {
                    try
                    {
                        this.DownloadMail(this.mailID);
                        Thread.Sleep(600000);
                    }
                    catch (Exception)
                    {
                    }
                    pluginDt = this.UpdateDateTime();
                    Thread.Sleep(600000);
                }
                Thread.Sleep(300000);
            }
        }
    }
    catch (Exception)
    {
        goto IL_00;
    }
}
```

encrypted localization

Hour check

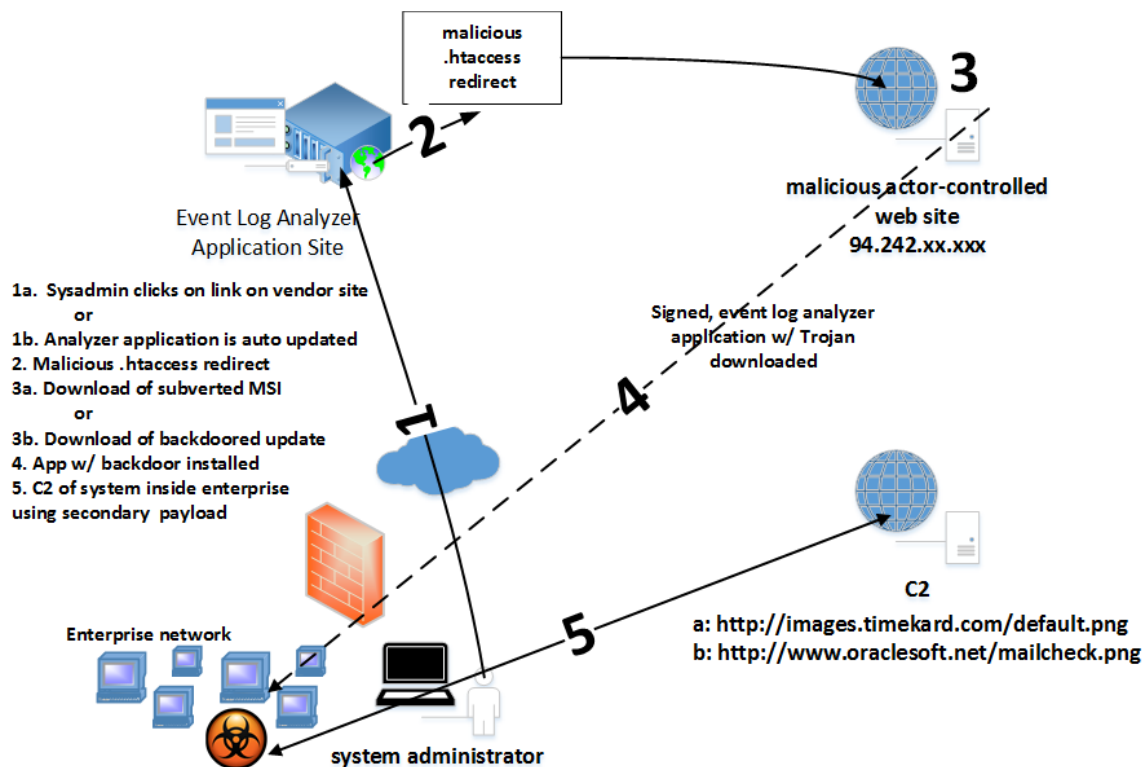
- ▶ The public Method Run checks the time and uses another encrypted string to set localization.
- ▶ The encrypted string decrypts to “Tokyo Standard Time” and will only run on Saturday, Tuesday, Thursday and Friday between 9pm and 9 am. The malware is hard coded to sleep 20 minutes (2 different 10 minute windows) between beacons.

Kingslayer supply chain attack

Contacted the developer of the Windows event log analysis application

Required adversary to have:

- ▶ Source code
- ▶ Code signing key/cert
- ▶ Administrative access to the update and download web sites



x64 malware w/ google-dash.com C2
submitted to VT **0**

Apr
5

google-dash.com lawfully seized &
sinkholed by RSA Research

Apr
7

office365e.com lawfully seized & sinkholed
by RSA Research

Apr
20

microsoft-cache.com, jbossass.org,
xjboss.com, ukoffering.com lawfully seized
and sinkholed by RSA Research

Apr
28

Schoolbell botnet peak of some 2,000
infections calling back to RSA Research

May
1

sinkholes

2016
Apr

supermanbox.org acquired & sinkholed by
RSA Research

May
31

Jun

Event log analysis software vendor
contacted, security notice posted

Jun
30

Jul

oraclesoft.net lawfully seized and sinkholed
by RSA Research

Jul
24

2016

Kingslayer victim verticals

US industrial manufacturer

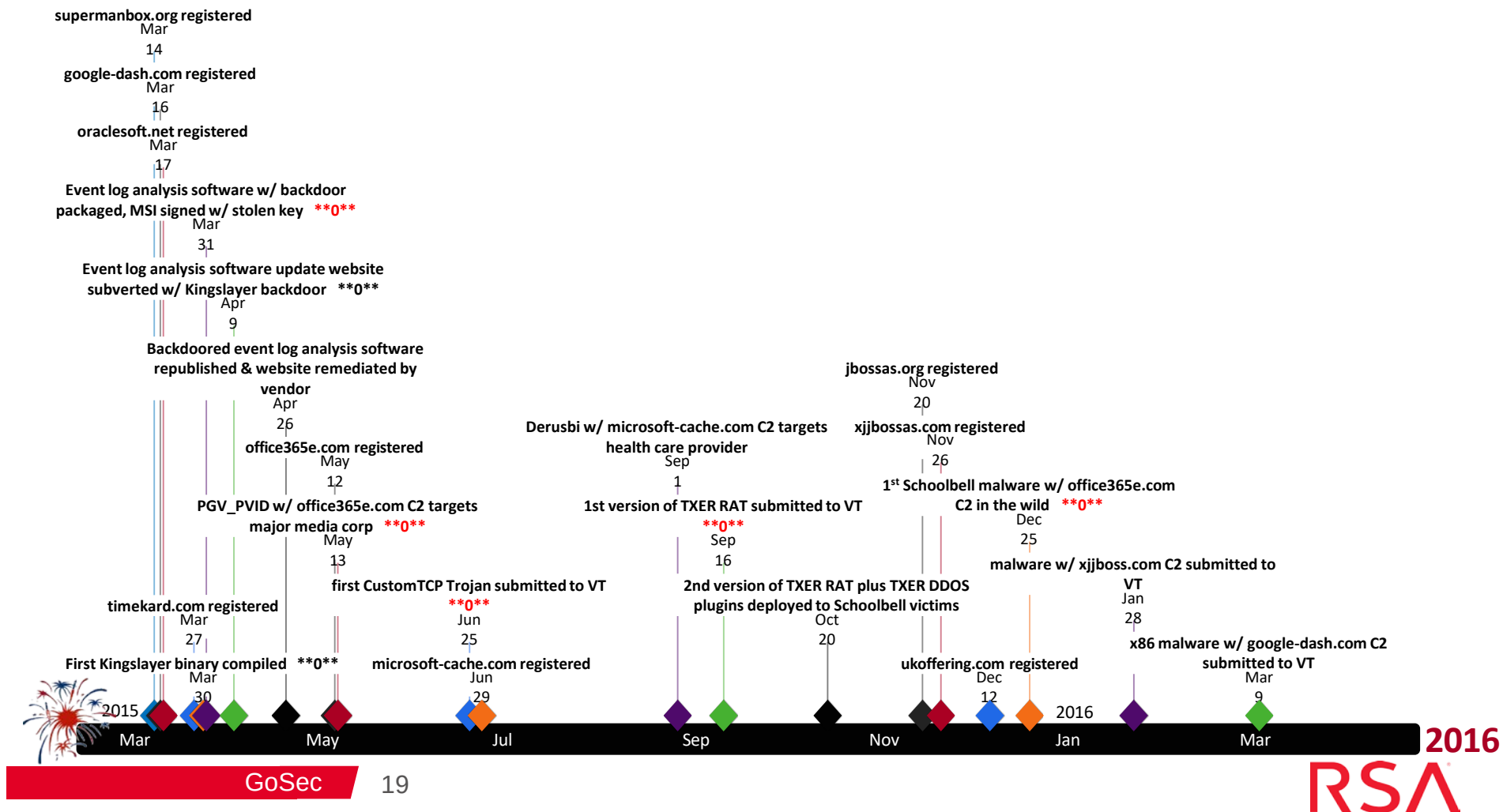
Canadian cleared defense contractor

US investment advisory firm

US construction engineering firm

US organization with redacted identity

Eastern European organization



Conclusion

- ▶ We observed sustained activity from an advanced threat actor group over 18+ months
- ▶ Evolutionary deployment of tools characterized by very low (if any) coverage by antivirus vendors
- ▶ Actors may be using Schoolbell as exploit/attack platform
- ▶ Actors used gradually shifting infrastructure) in their strategic targeting (Kingslayer) that was linked to broad exploitation activity (Schoolbell)
- ▶ Aimed at sysadmins, the specific target of Kingslayer is unknown
- ▶ It takes keen visibility and awareness to discover advanced threat activity like a supply chain attack

The screenshot shows the VirusTotal analysis page for a file named 'Service.exe'. The file's SHA256 hash is 7aa474d0d39a41768149f413c451e9208f73af4d262b6575ada31644f5699153. The detection ratio is 0 / 51, and the analysis date is 2016-07-01 01:10:43 UTC (1 month, 4 weeks ago). A green bar at the top indicates 'Probably harmless! There are strong indicators suggesting that this file is safe to use.' Below this, the 'File identification' section lists various hashes and file types. The 'Virus Total metadata' section at the bottom shows the first submission on 2015-04-17 and the last submission on 2016-07-01.

File identification	
MD5	f97a2744a4964044c60ac241f92e05d7
SHA1	b22f72b4a5bb33f7ea934cb4b443882fe7f556
SHA256	7aa474d0d39a41768149f413c451e9208f73af4d262b6575ada31644f5699153
ssdeep	768 j0bwDCz9Emxt8wNOqr13stHGZGgEeU8/DWiyasX71r5Oa74O1j0zxtFedViyDq7Oa74K
authentihash	0bcd14267bdc2a5a743eb9df97fc21d6673d316b30cb4c7fd80350da0d02856
imphash	f34d5f2d4577ed6d9ceec516c1f5a744
File size	41.1 KB (42088 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly
TrID	Win64 Executable (generic) (64.6%) Win32 Dynamic Link Library (generic) (15.3%) Win32 Executable (generic) (10.5%) Generic Win/DOS Executable (4.6%) DOS Executable Generic (4.6%)

Virus Total metadata	
First submission	2015-04-17 13:21:41 UTC (1 year, 4 months ago)
Last submission	2016-07-01 01:10:43 UTC (1 month, 4 weeks ago)



Thank You

Special thanks:

Chuck Helstein, DigitalOcean

Darien Huss, Proofpoint

Luis Garcia of luisangelgarcia.com

MS-ISAC for notification assistance

CCIRC for notification assistance

Unnamed researchers with whom we work daily

kent.backman@rsa.com

RSA