

RSA® Conference 2015

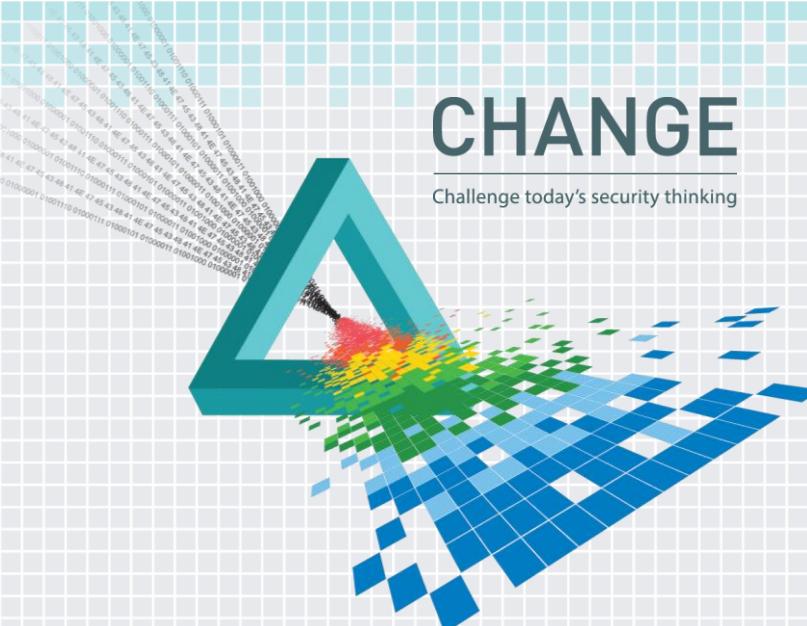
San Francisco | April 20-24 | Moscone Center

SESSION ID: ANF-R01

Notice of Eviction

Phil F. Burdette

Sr. Security Researcher
Dell SecureWorks Counter Threat Unit – Special Operations
@burdtep



CHANGE

Challenge today's security thinking

Objective

- ◆ To challenge incident responders to *change* the way we approach incident response evictions by studying our adversaries' responses to stimuli



SecureWorks

Eviction Strategies

- ◆ Ad Hoc – playing whack-a-mole
- ◆ Containment – restricting assets or access points
- ◆ Compartmented – remediating segments
- ◆ Failover – executing disaster recovery plan
- ◆ Full Scope – hunting for access points

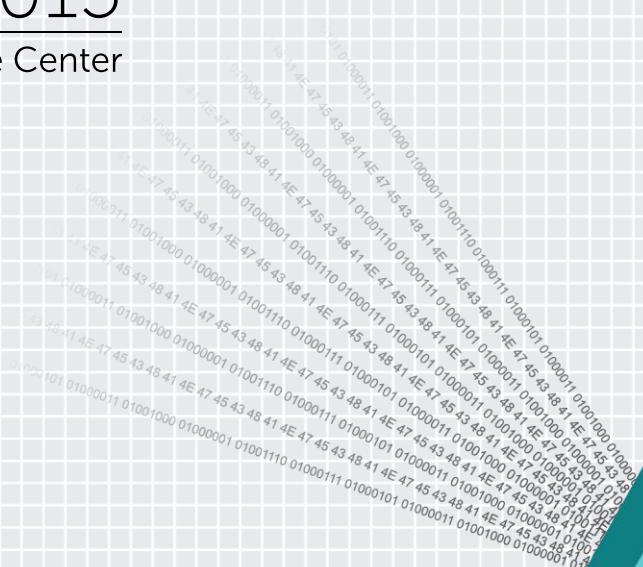
Eviction Strategies

- ◆ Ad Hoc – playing whack-a-mole
- ◆ Containment – restricting assets or access points
- ◆ Compartmented – remediating segments
- ◆ Failover – implementing disaster recovery plan
- ◆ Full Scope – hunting for access points

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

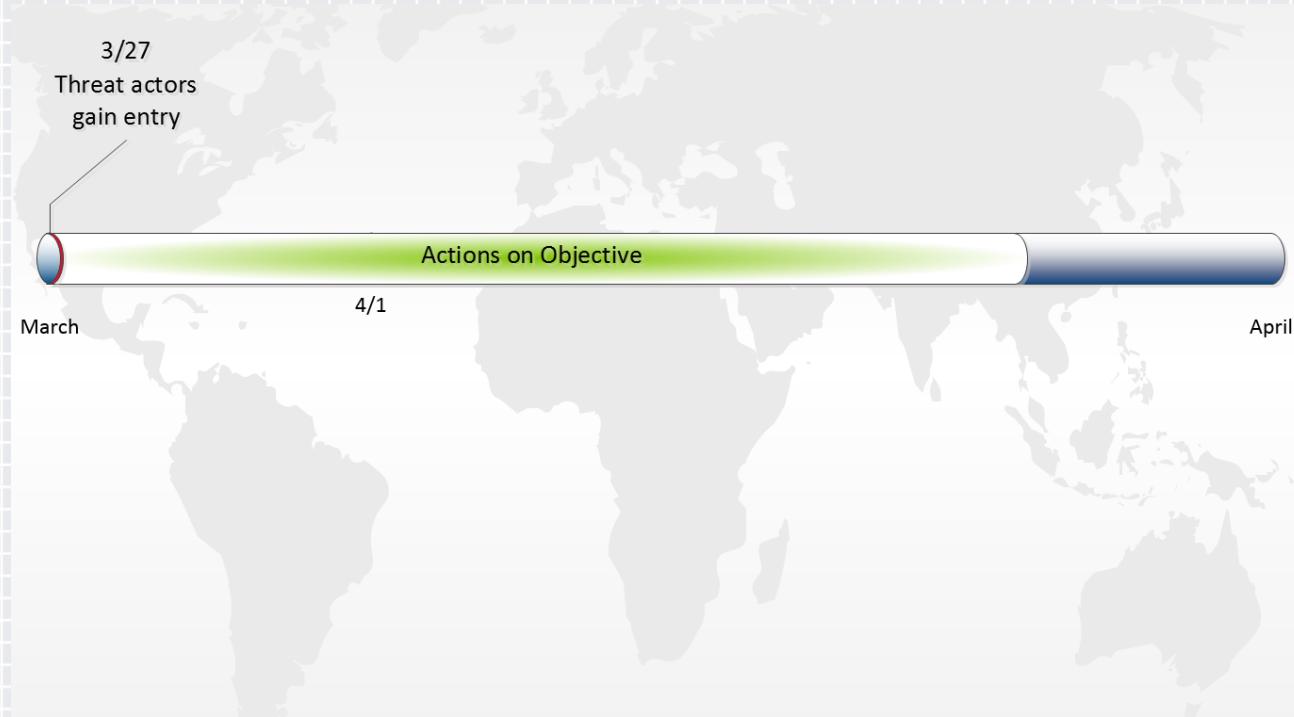
Ad Hoc Eviction



#RSAC

Ad Hoc Eviction

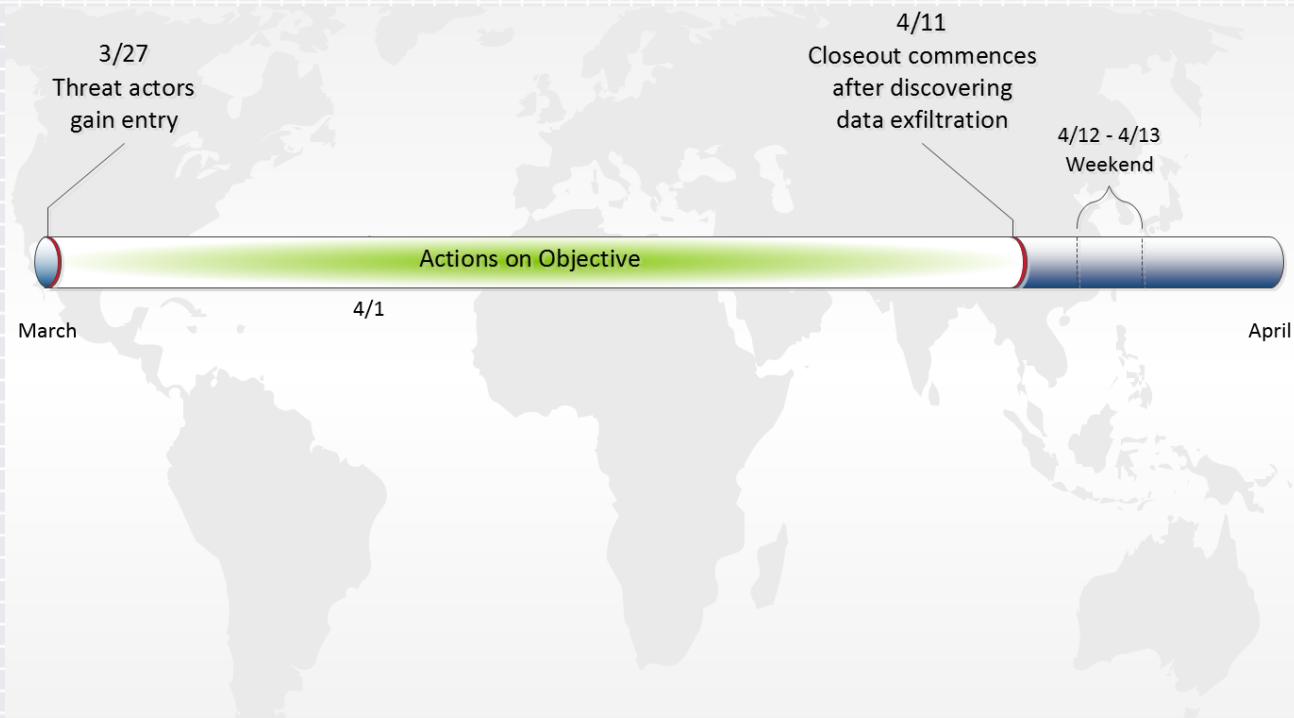
TG-1588



SecureWorks

Ad Hoc Eviction

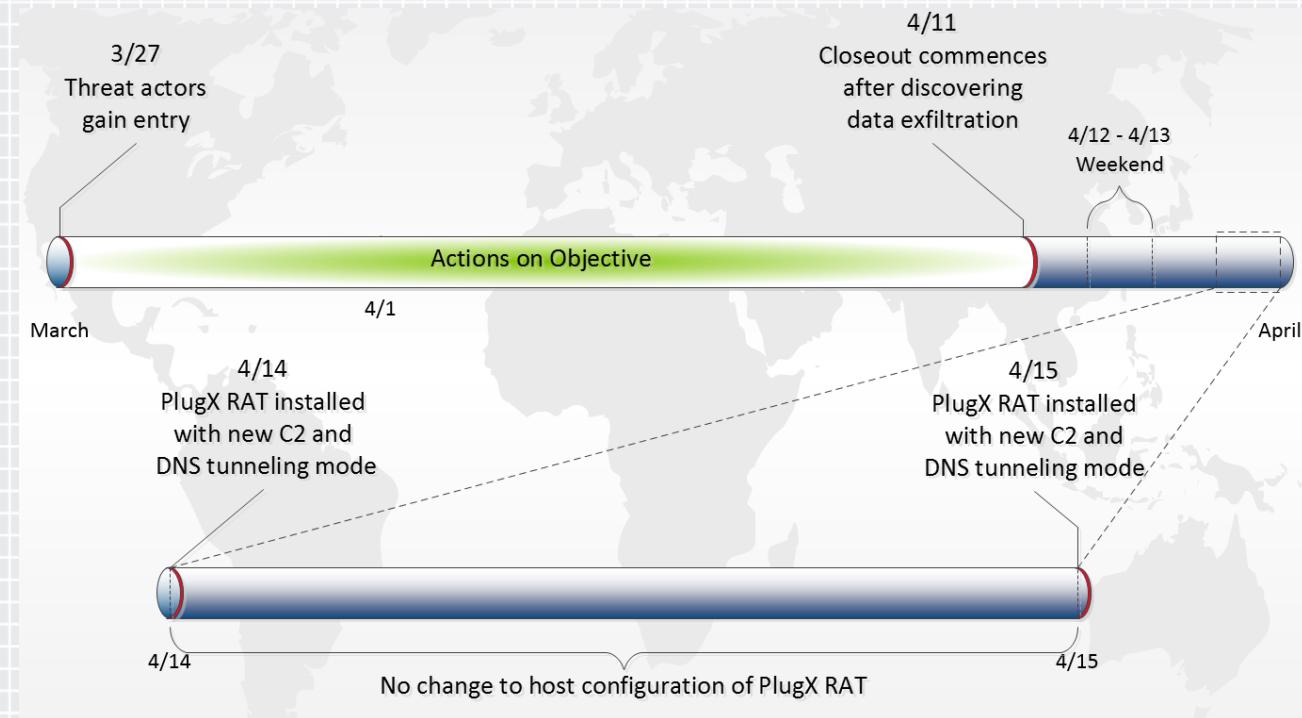
TG-1588



SecureWorks

Ad Hoc Eviction

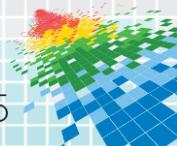
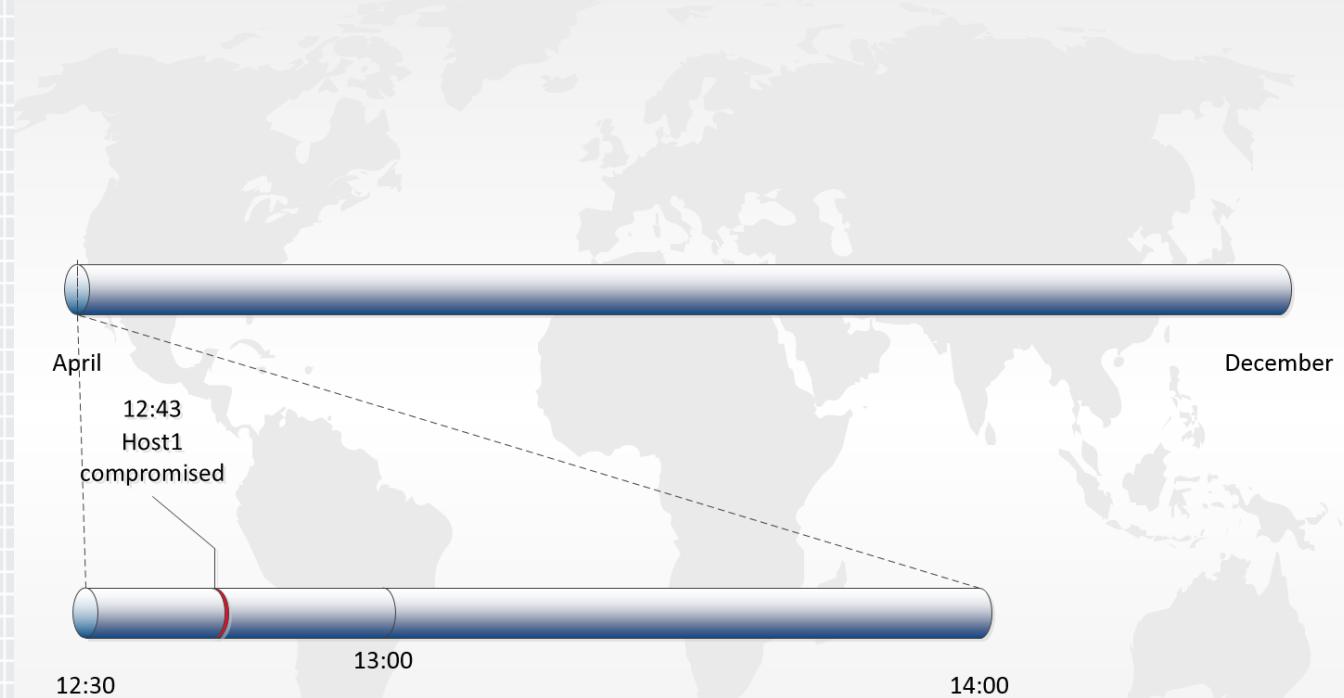
TG-1588



SecureWorks

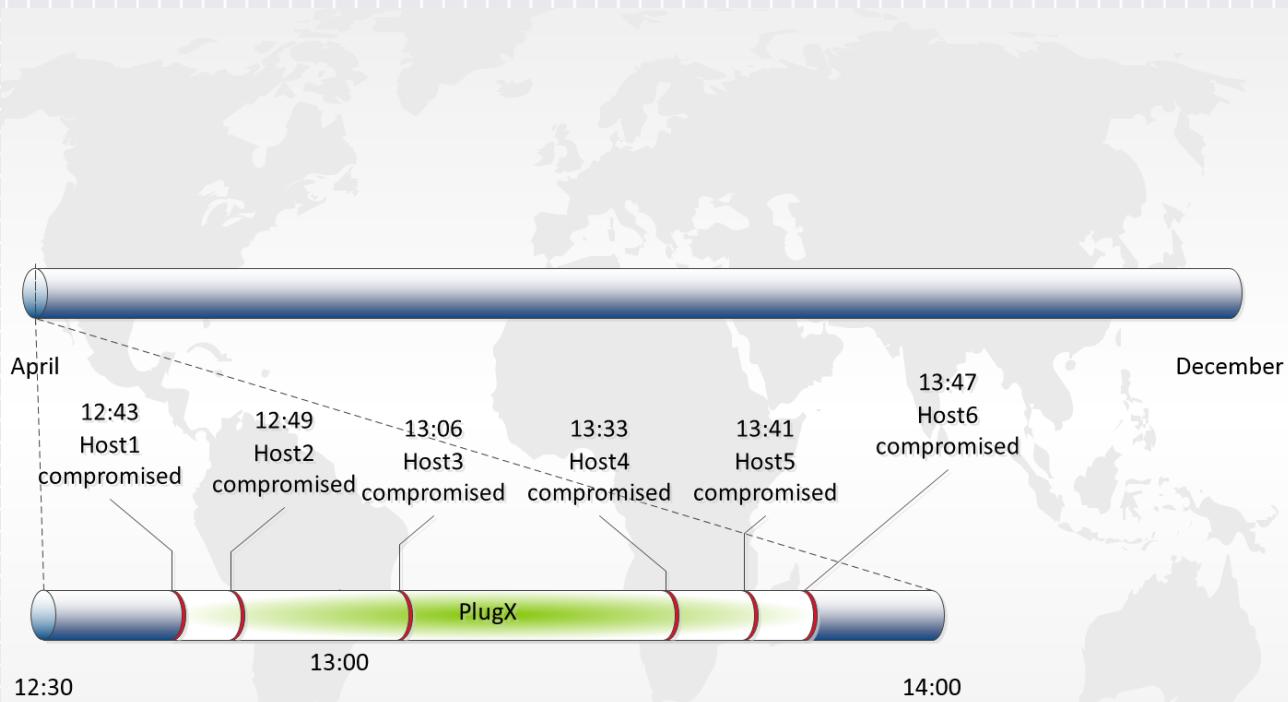
Ad Hoc Eviction

TG-3390



Ad Hoc Eviction

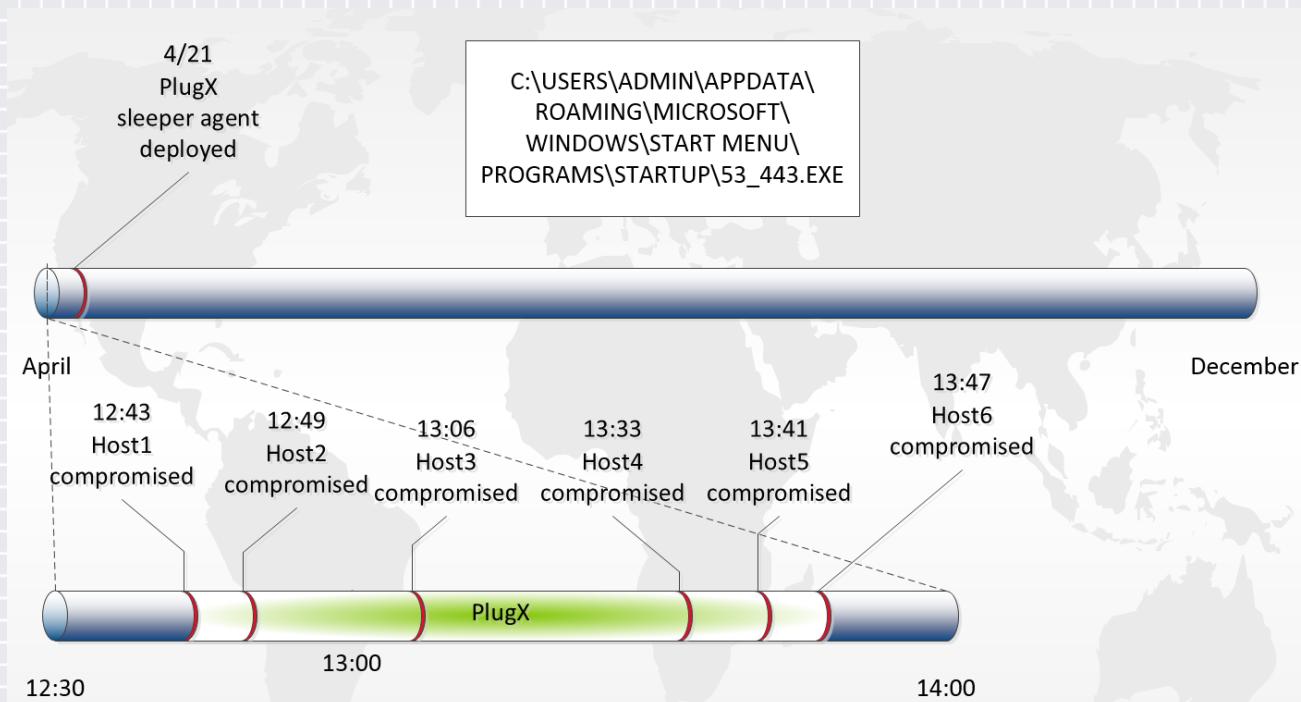
TG-3390



SecureWorks

Ad Hoc Eviction

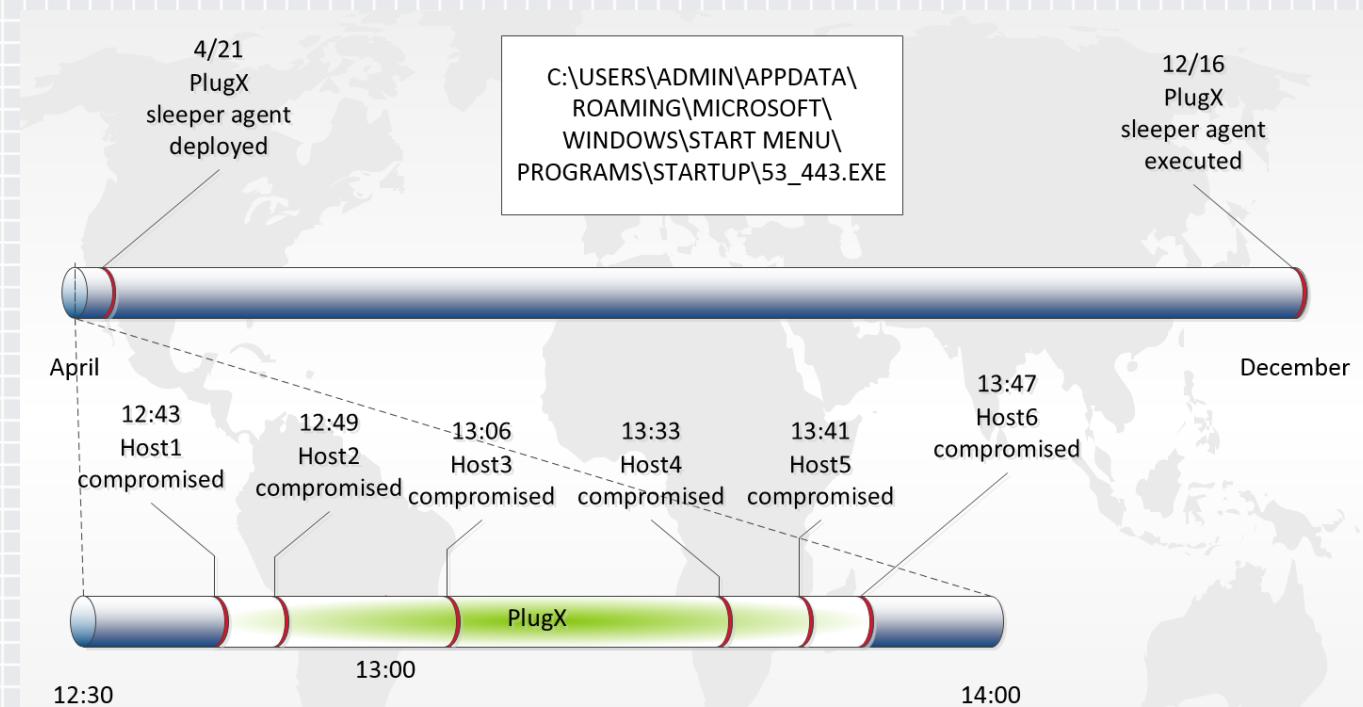
TG-3390



SecureWorks

Ad Hoc Eviction

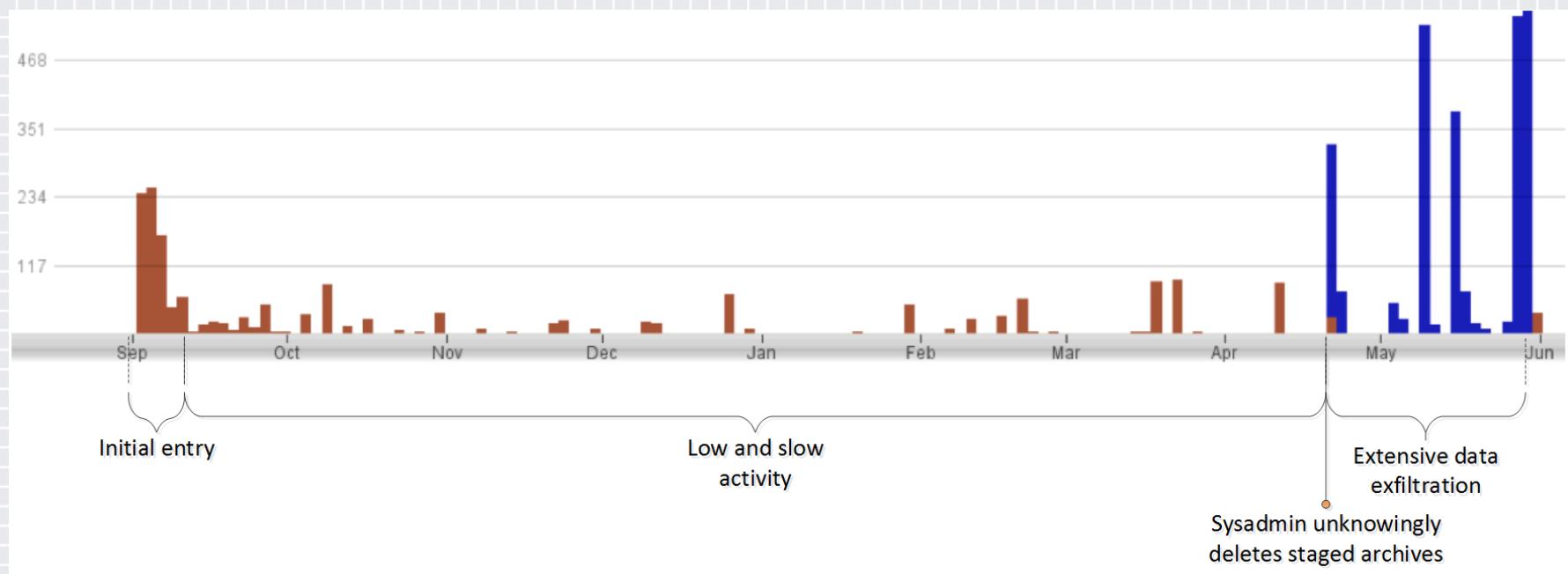
TG-3390



SecureWorks

Ad Hoc Eviction

TG-3301

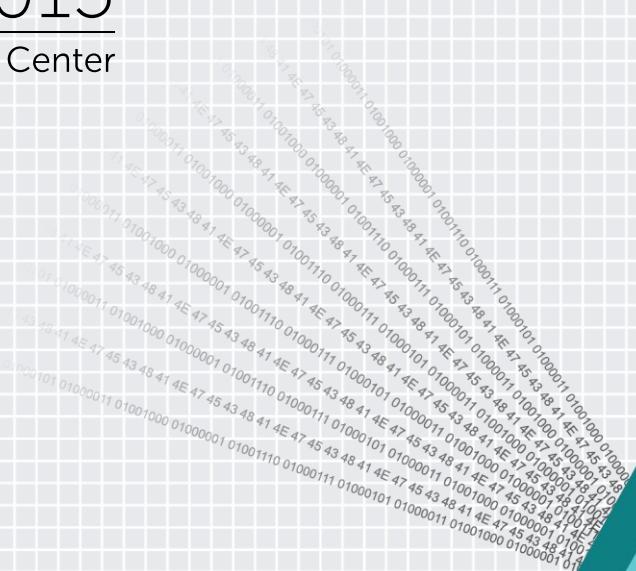


SecureWorks



San Francisco | April 20-24 | Moscone Center

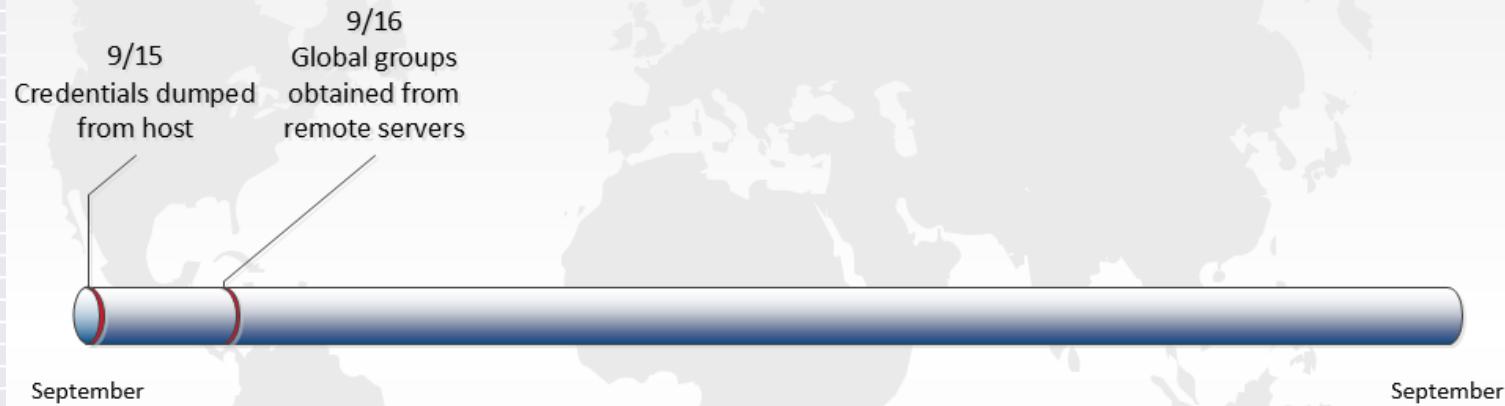
Containment Eviction



#RSAC

Containment Eviction

TG-0416



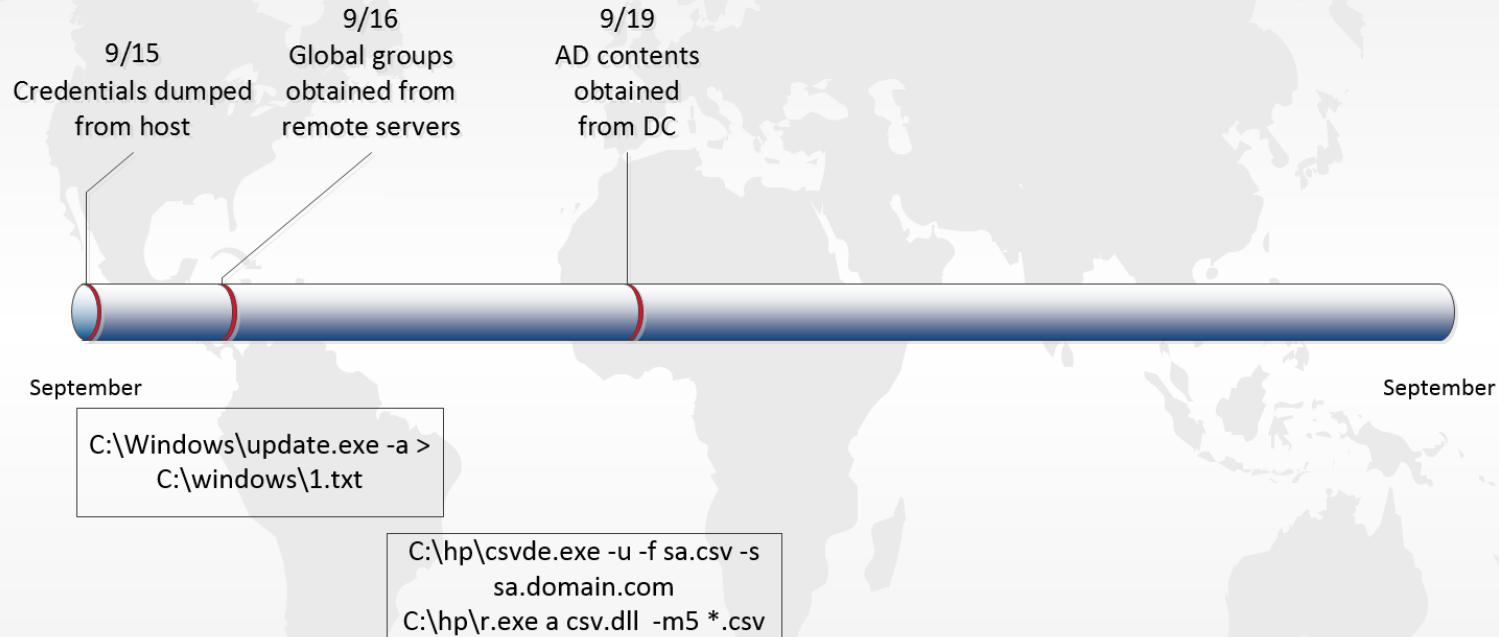
```
C:\Windows\update.exe -a >  
C:\windows\1.txt
```



SecureWorks

Containment Eviction

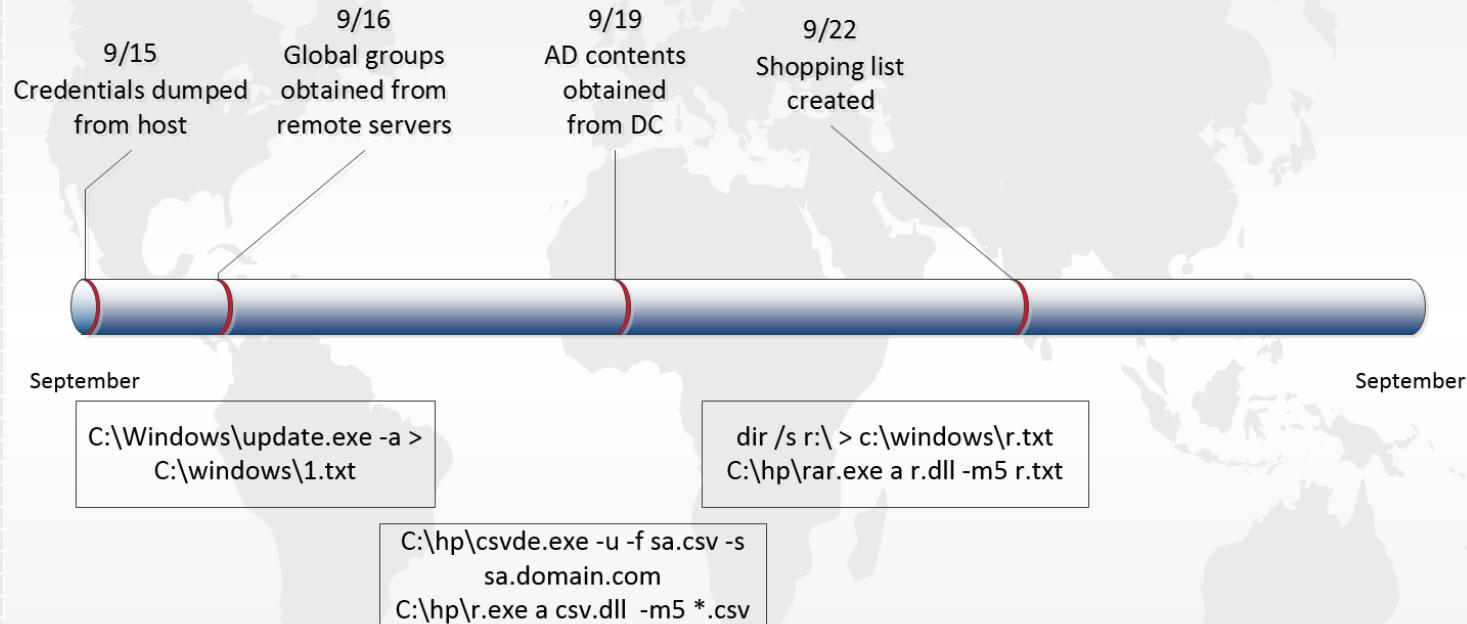
TG-0416



SecureWorks

Containment Eviction

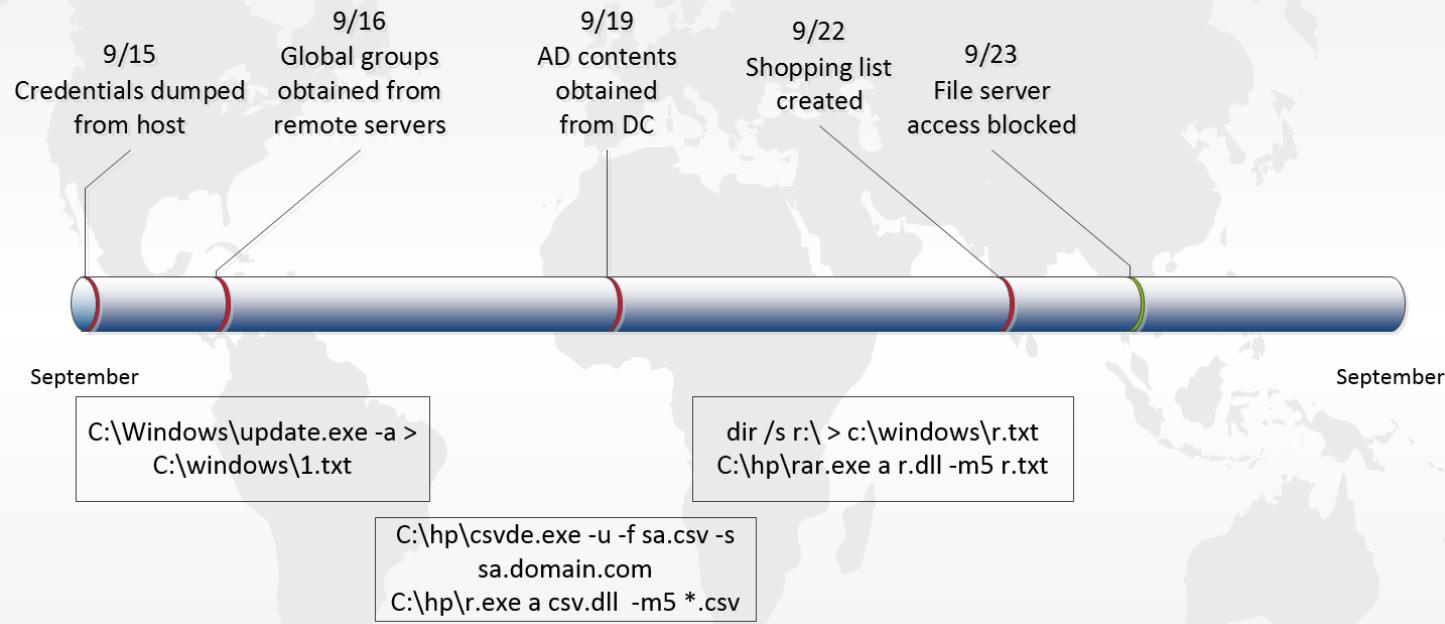
TG-0416



SecureWorks

Containment Eviction

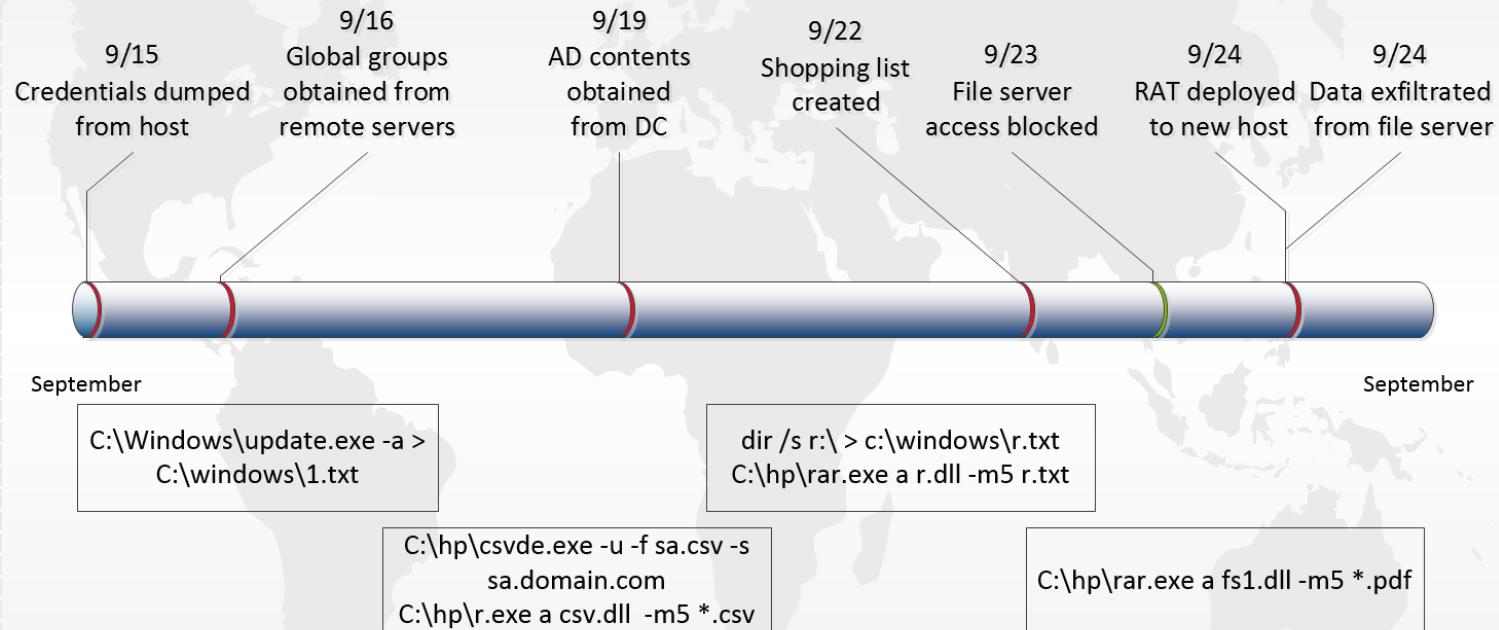
TG-0416



SecureWorks

Containment Eviction

TG-0416

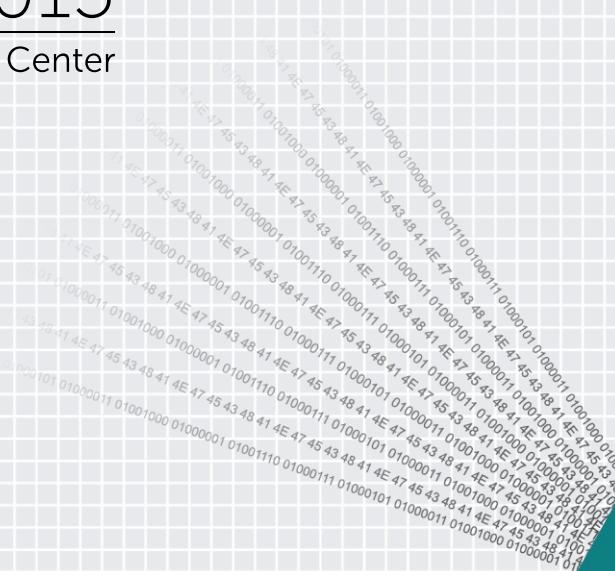


SecureWorks

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Full-Scope Eviction



Full-Scope Eviction

TG-3390

01:10 - 01:25

External recon using
google.co.jp to find
remote access solutions



01:00

06:00

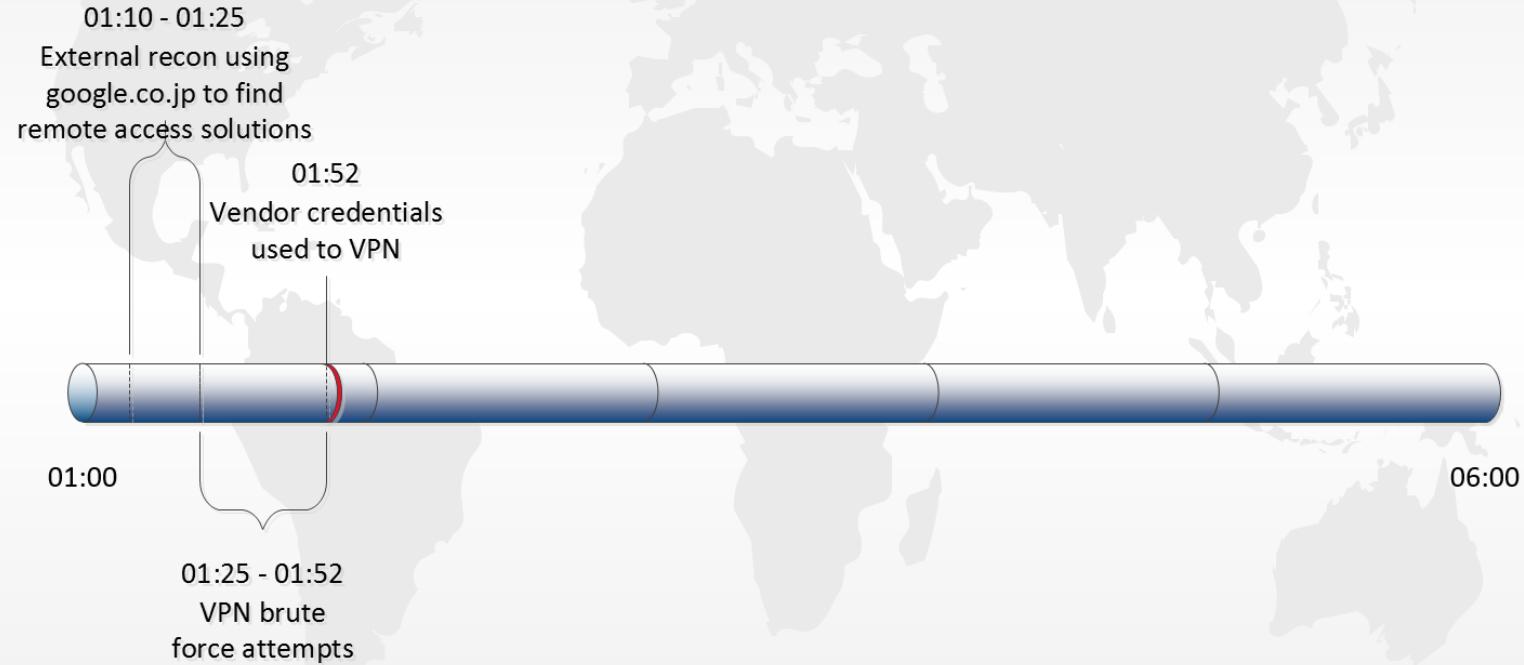


SecureWorks



Full-Scope Eviction

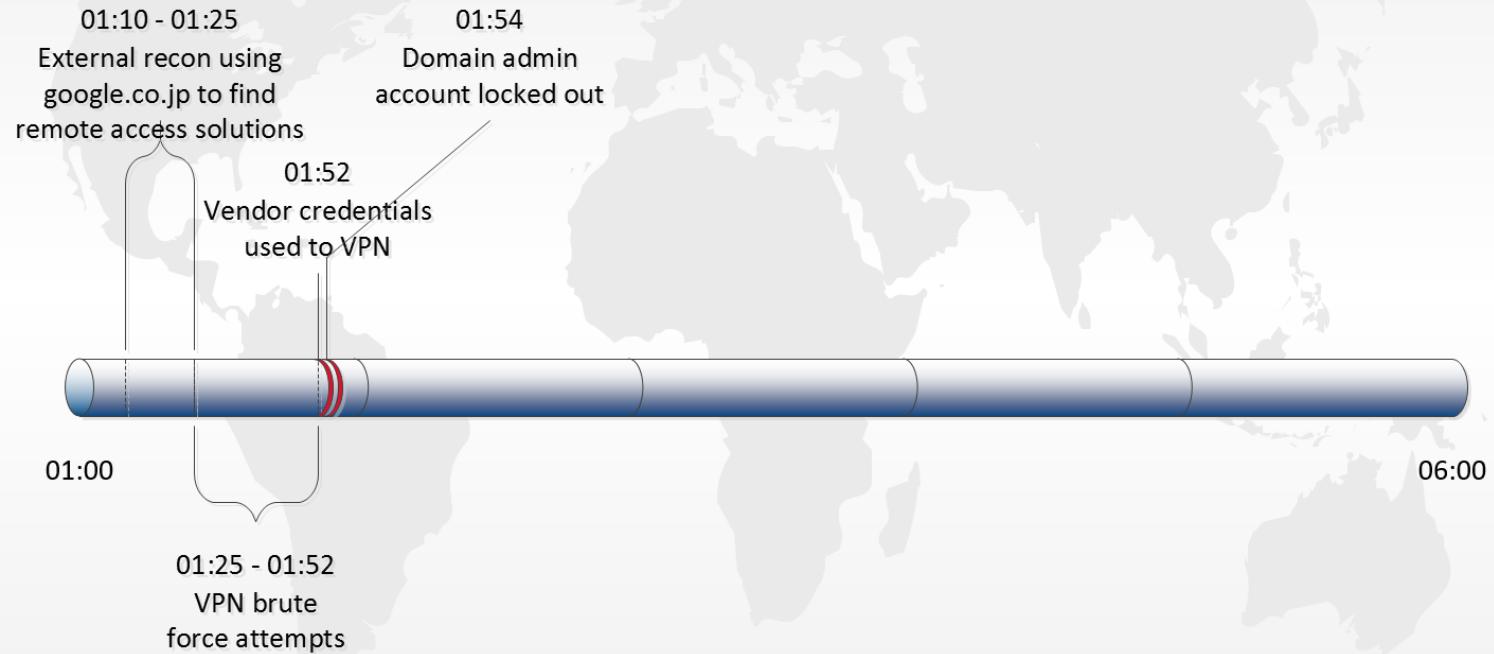
TG-3390



SecureWorks

Full-Scope Eviction

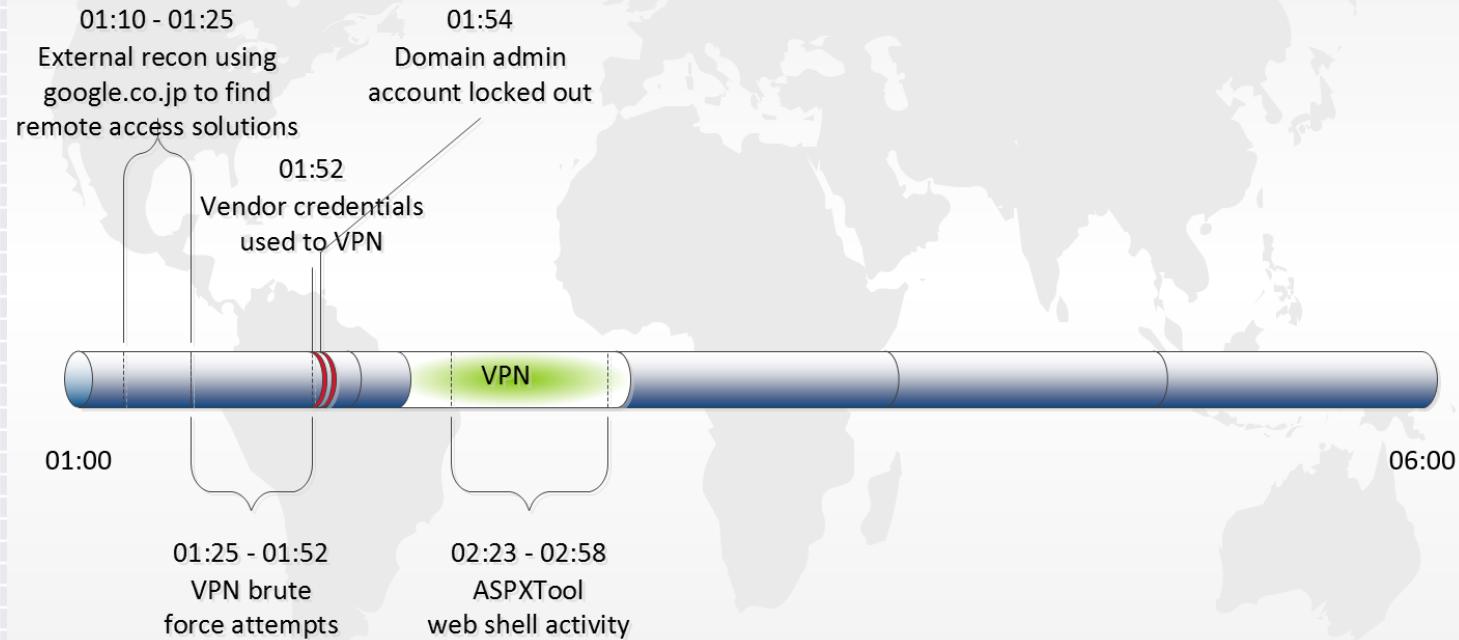
TG-3390



SecureWorks

Full-Scope Eviction

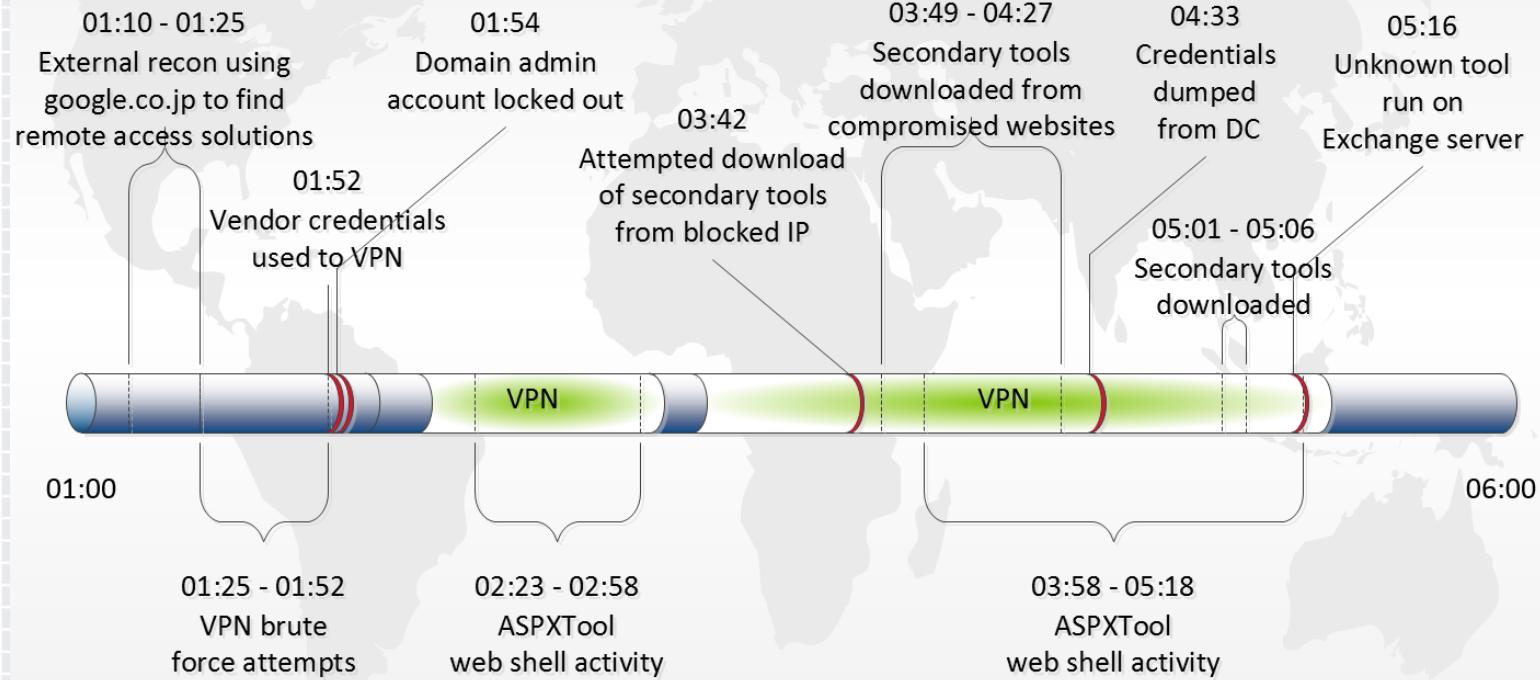
TG-3390



SecureWorks

Full-Scope Eviction

TG-3390



SecureWorks

Full-Scope Eviction

TG-1314

9/11
PHP vulnerability
exploited to
gain entry



September

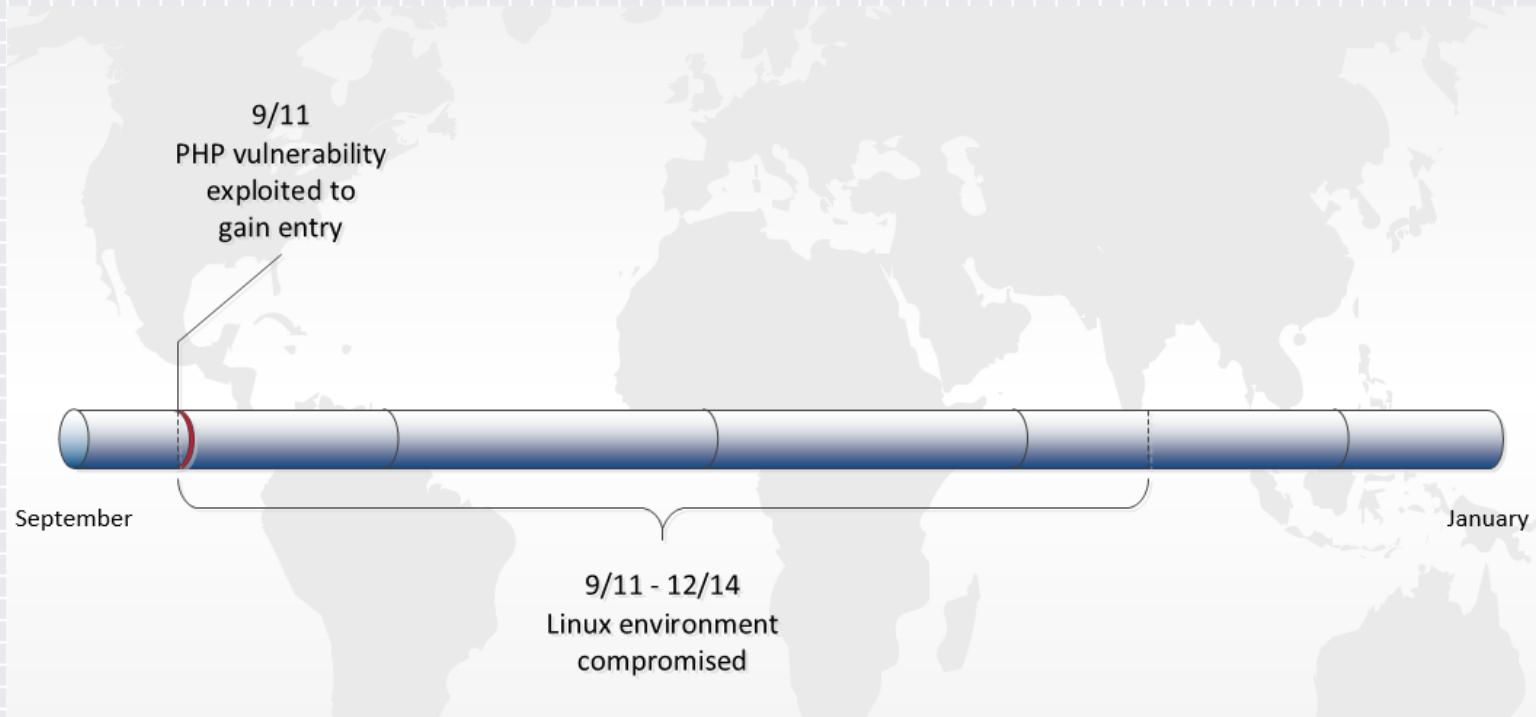
January



SecureWorks

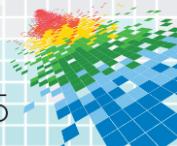
Full-Scope Eviction

TG-1314



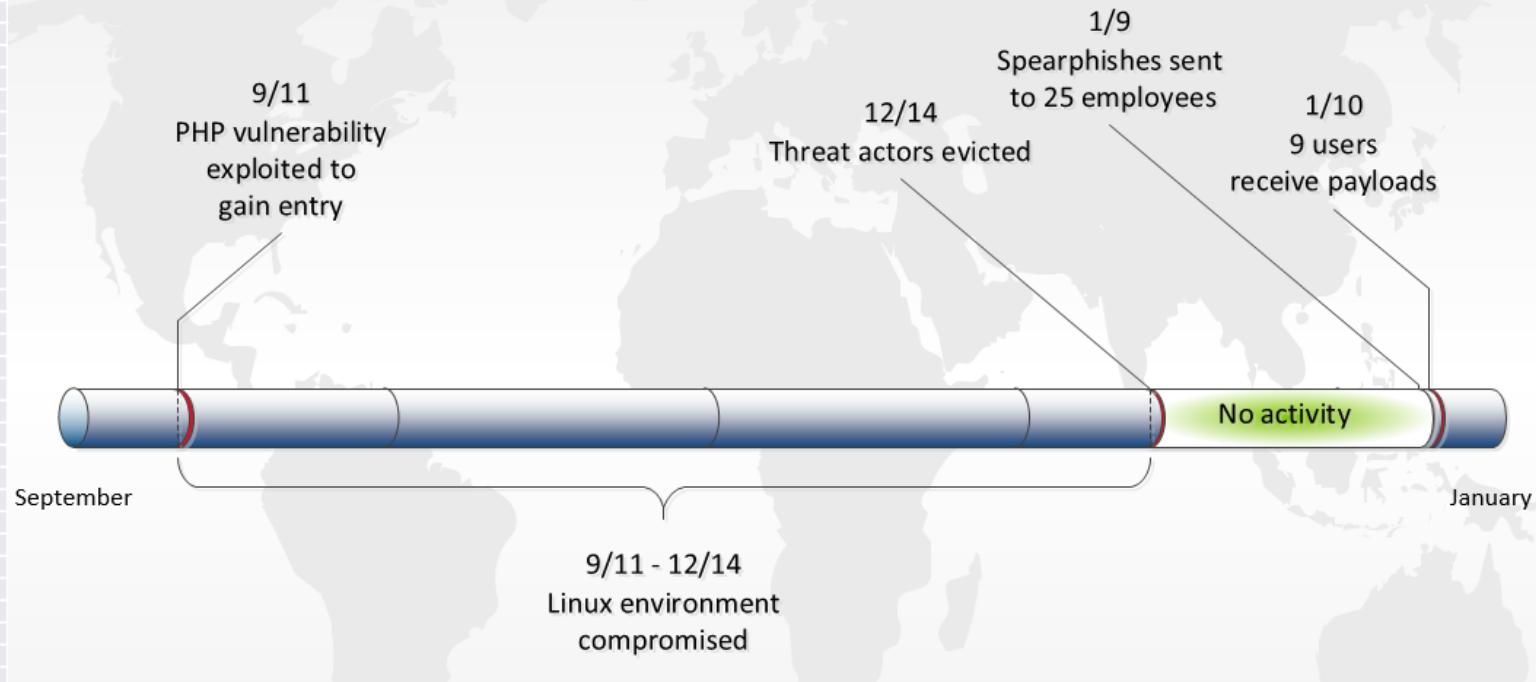
Full-Scope Eviction

TG-1314



Full-Scope Eviction

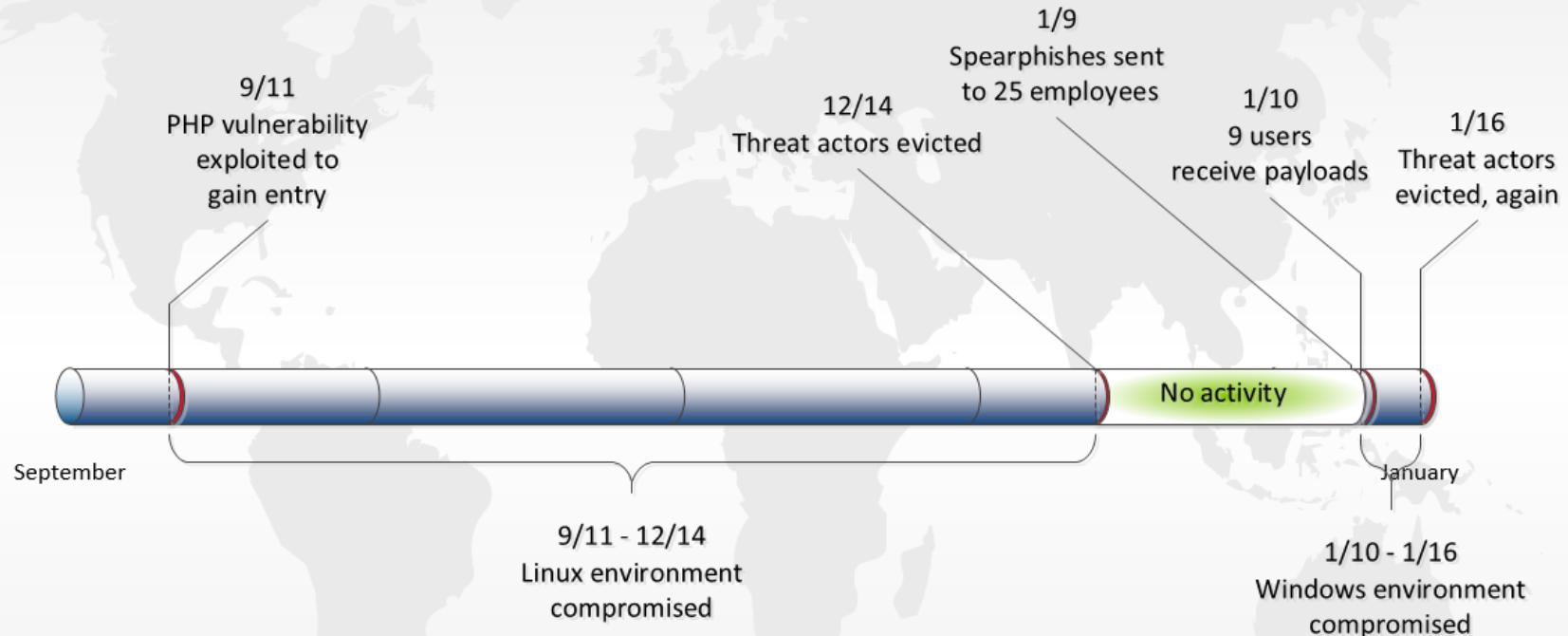
TG-1314



SecureWorks

Full-Scope Eviction

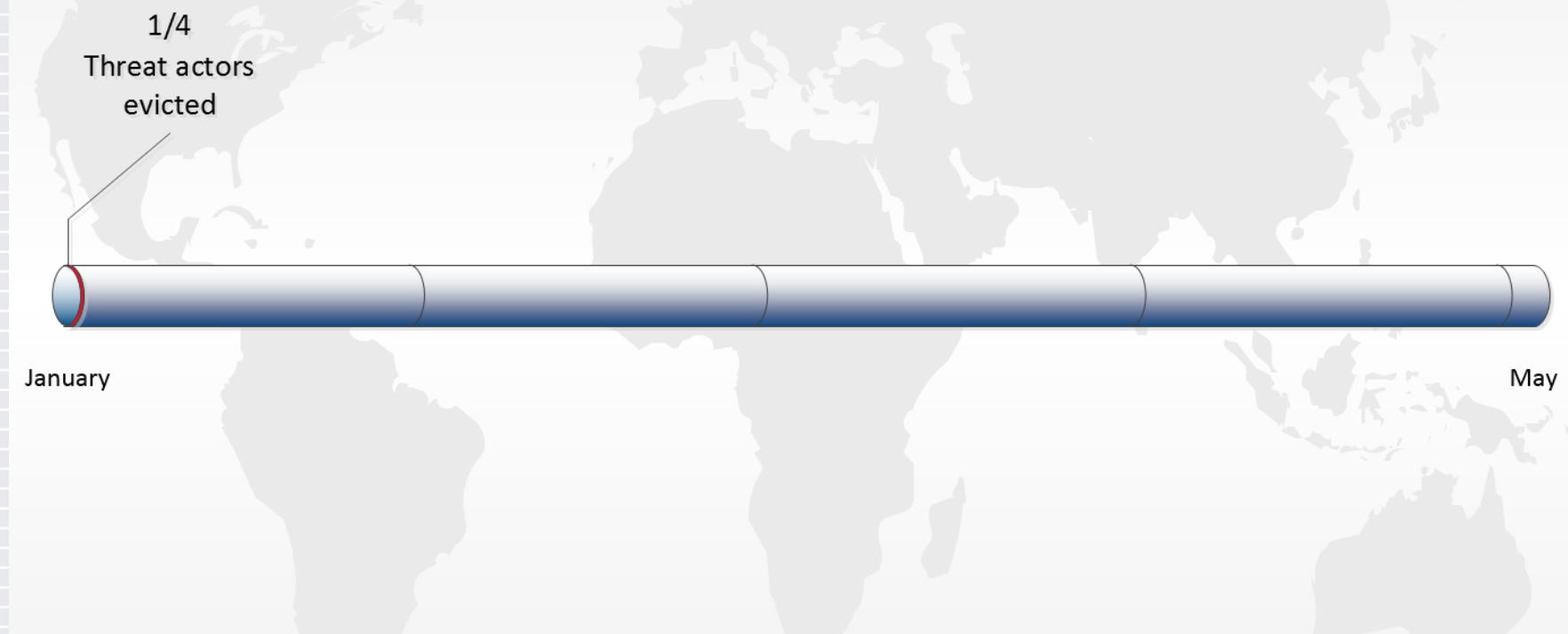
TG-1314



SecureWorks

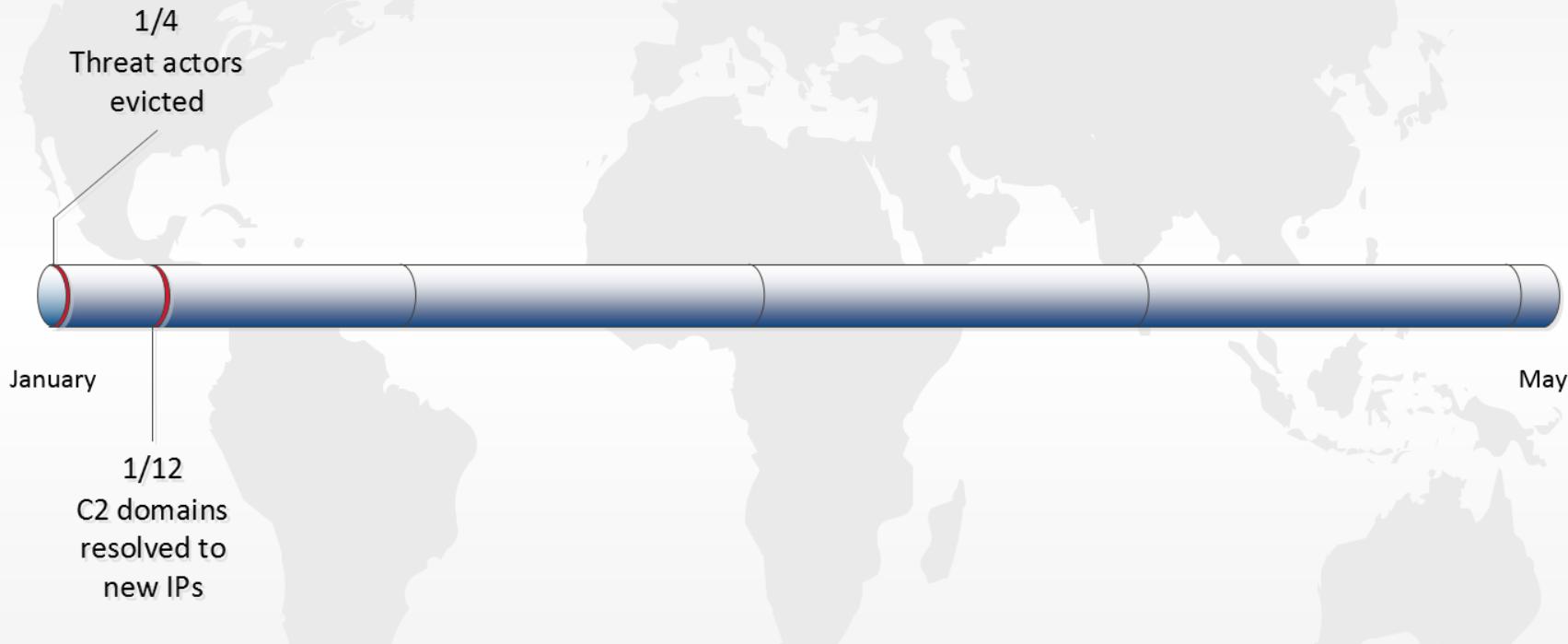
Full-Scope Eviction

TG-1588



Full-Scope Eviction

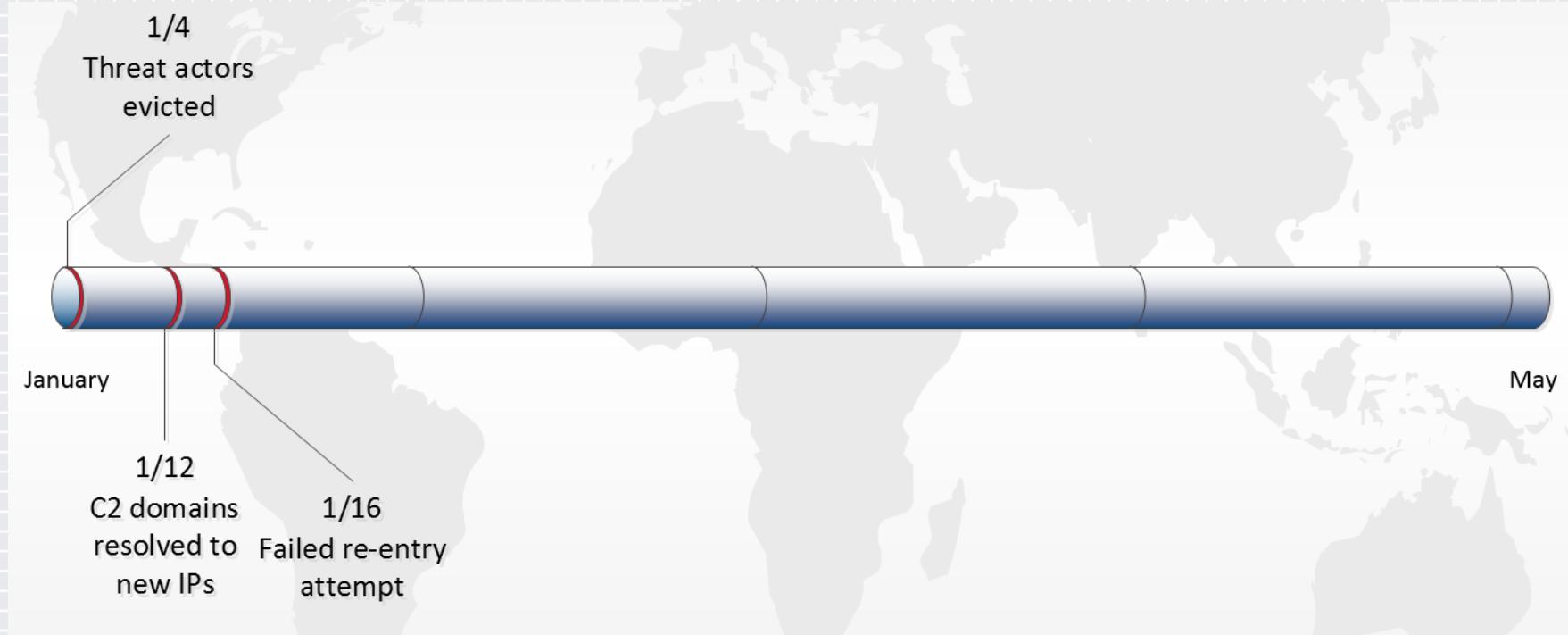
TG-1588



SecureWorks

Full-Scope Eviction

TG-1588



SecureWorks

Full-Scope Eviction

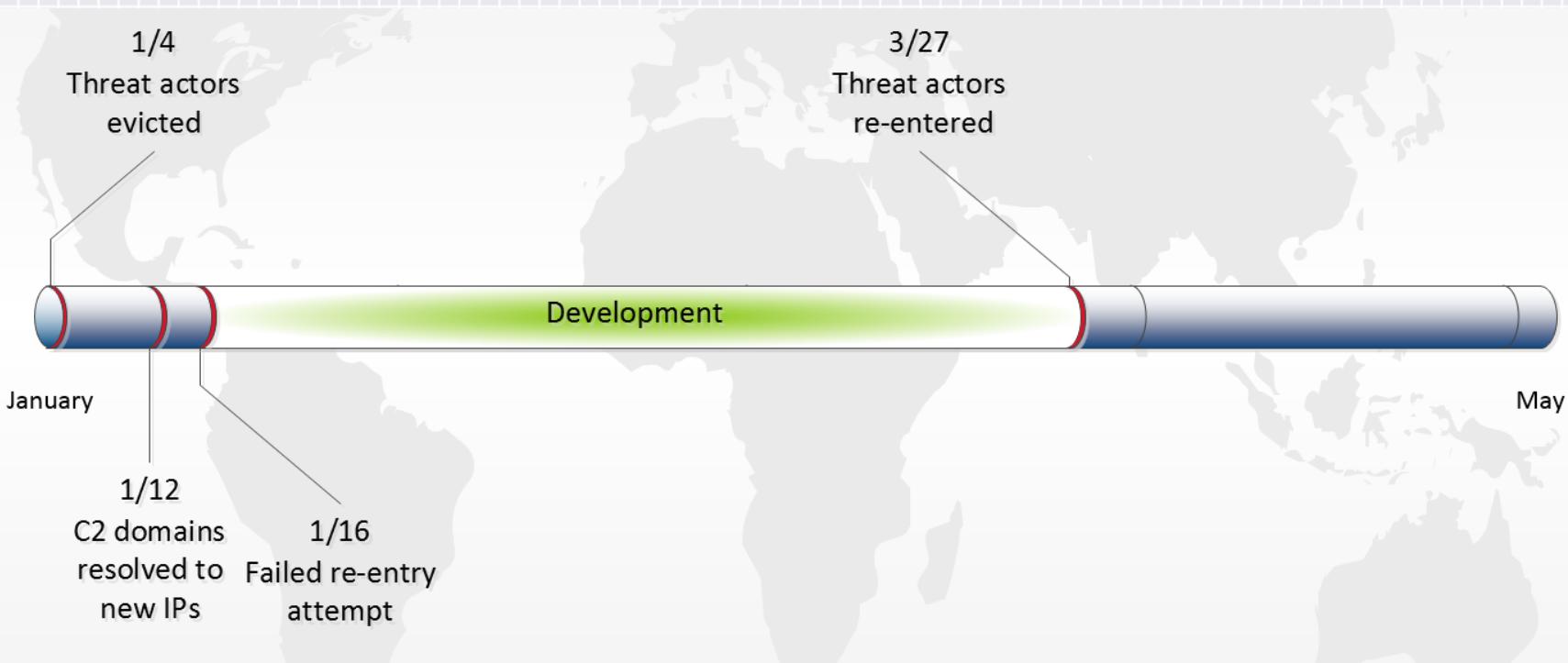
TG-1588



SecureWorks

Full-Scope Eviction

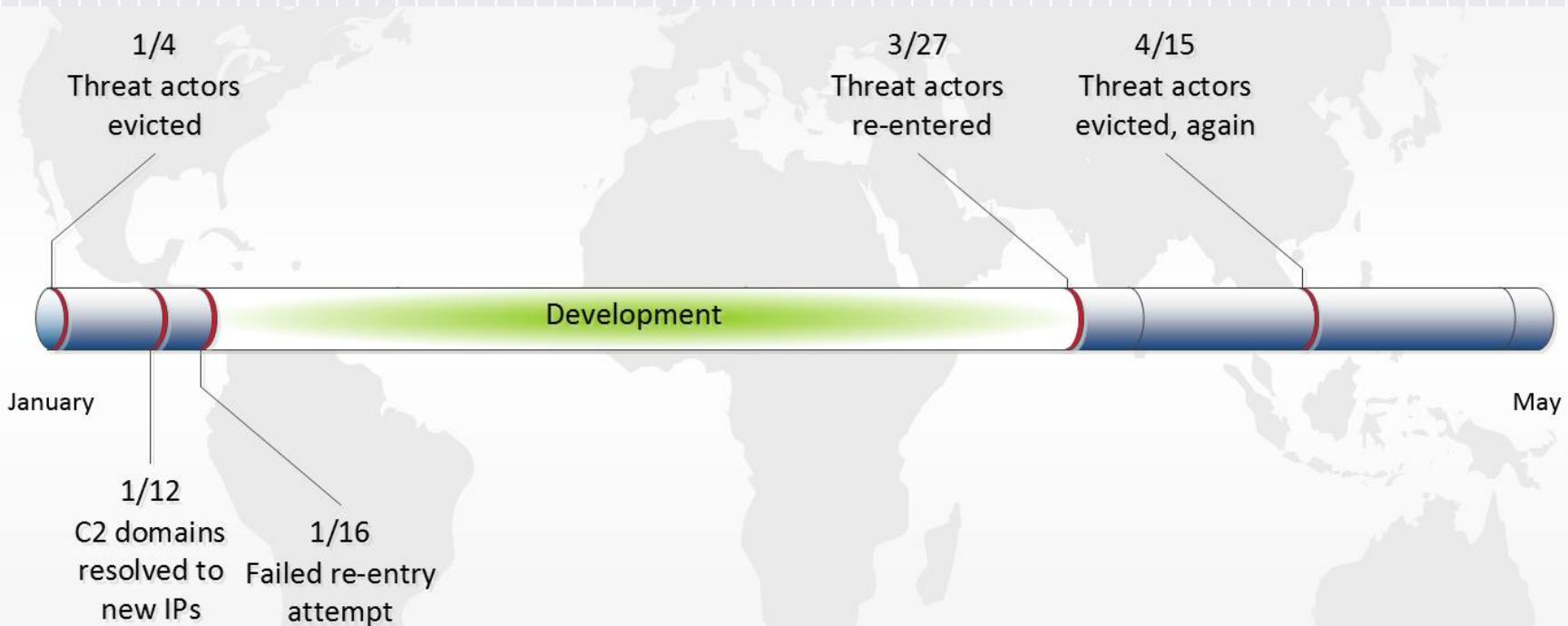
TG-1588



SecureWorks

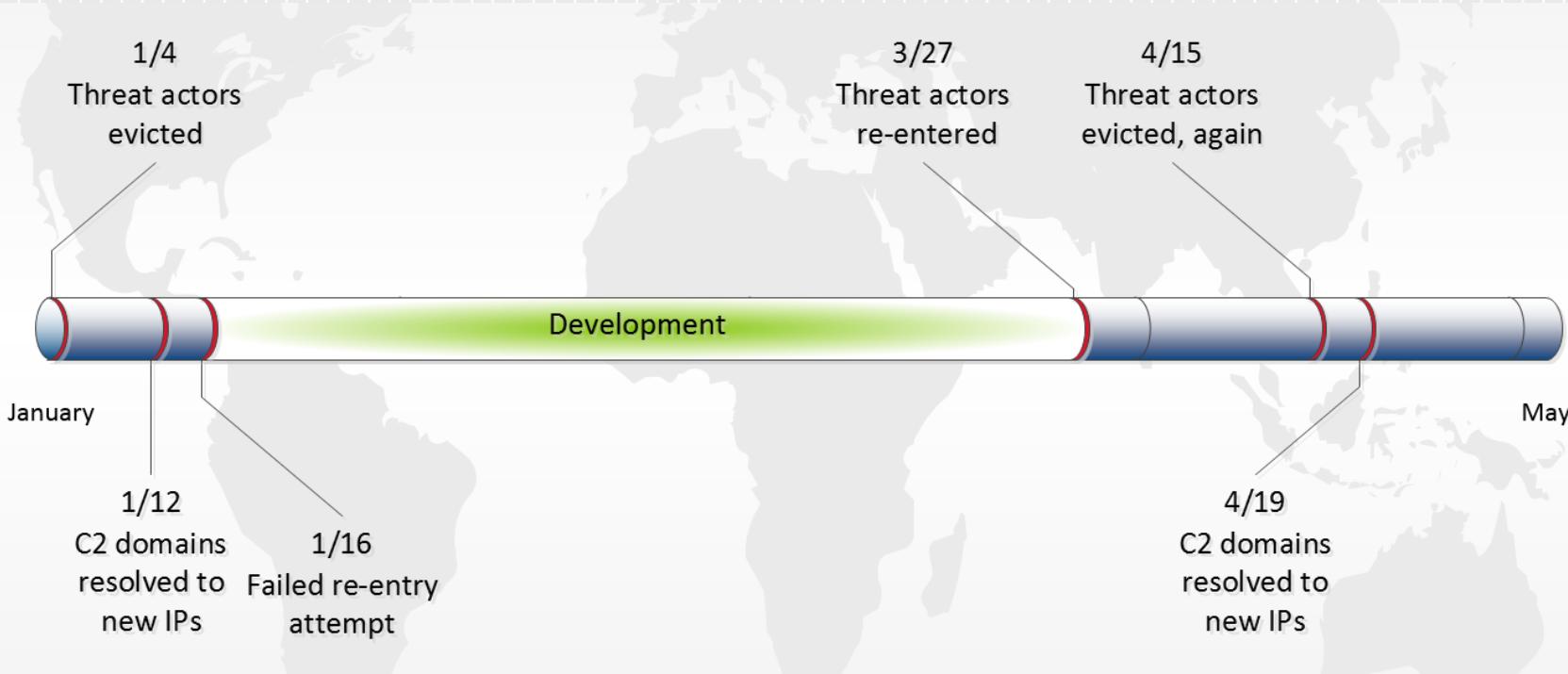
Full-Scope Eviction

TG-1588



Full-Scope Eviction

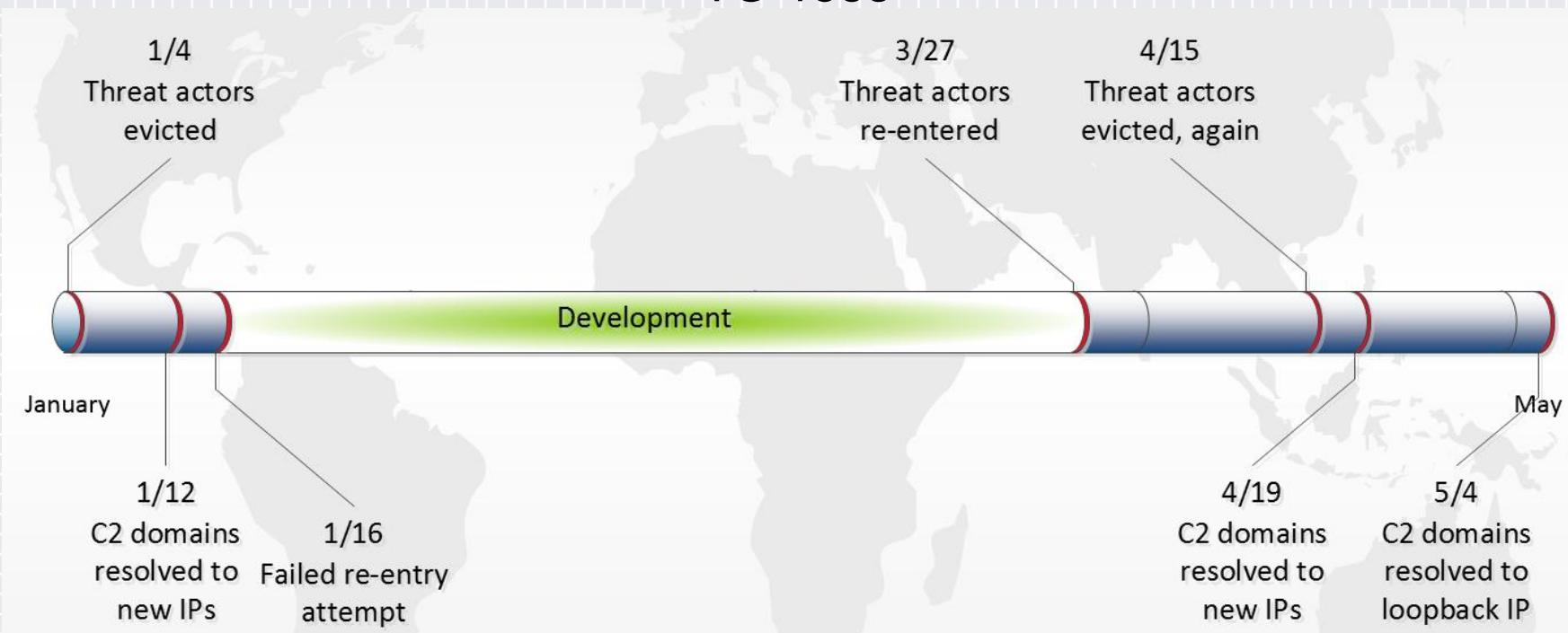
TG-1588



SecureWorks

Full-Scope Eviction

TG-1588



SecureWorks

Lessons Learned

- ◆ Incident response is often a marathon, not a sprint
- ◆ Apply Occam's razor
- ◆ Conduct root cause analysis
- ◆ Don't throw the first punch unless you have a plan to win
- ◆ Weekends are your friend
- ◆ Order of execution for eviction steps is important



Conclusion

- ◆ Implement and practice targeted threat response plan
- ◆ Accurately assess the threat and the risk to determine best eviction strategy
 - ◆ Ad-Hoc
 - ◆ Containment
 - ◆ Compartmented
 - ◆ Failover
 - ◆ Full Scope
- ◆ Improving defense = reducing time to detect and effort to respond



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Thank You

