RSAConference2015
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
@burdetp

Objective

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

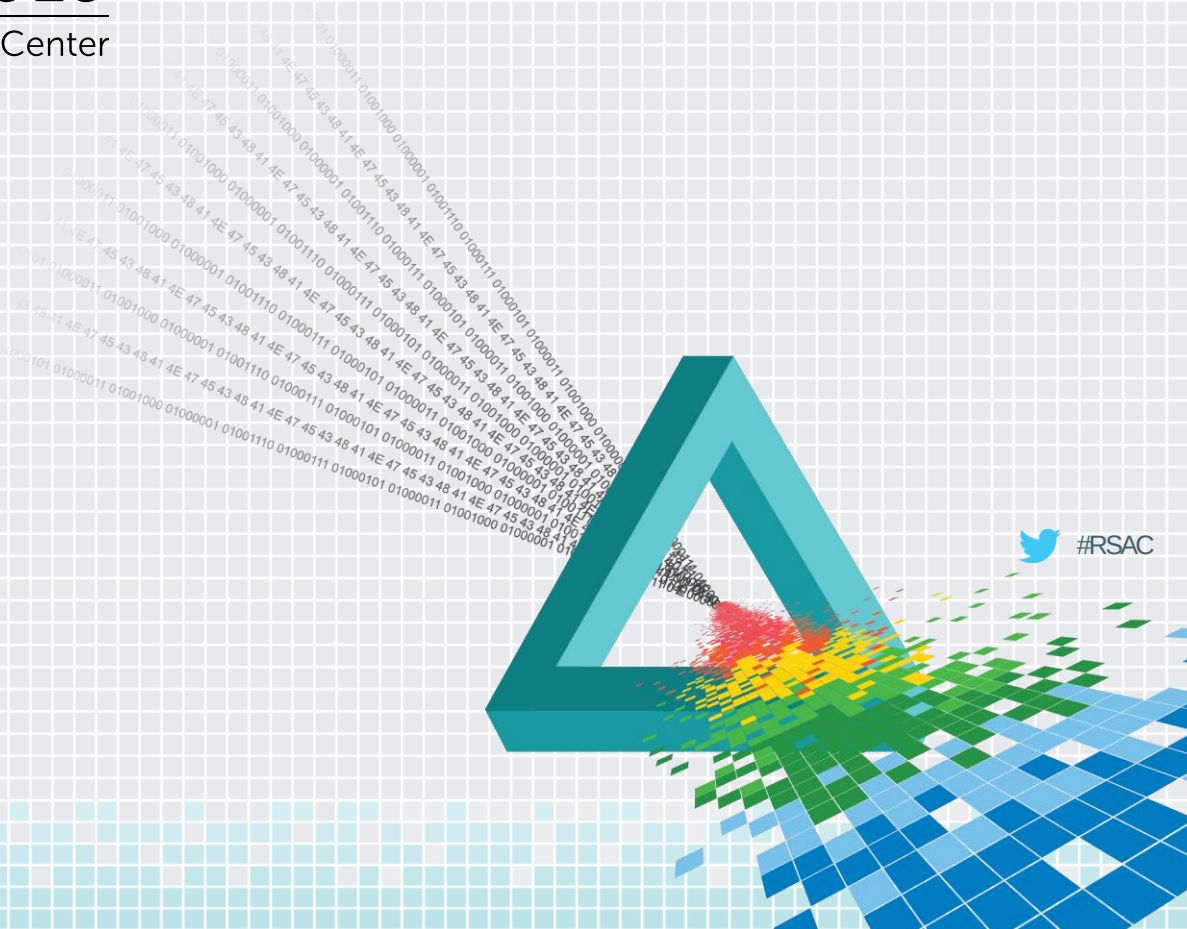
Eviction Strategies

- 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

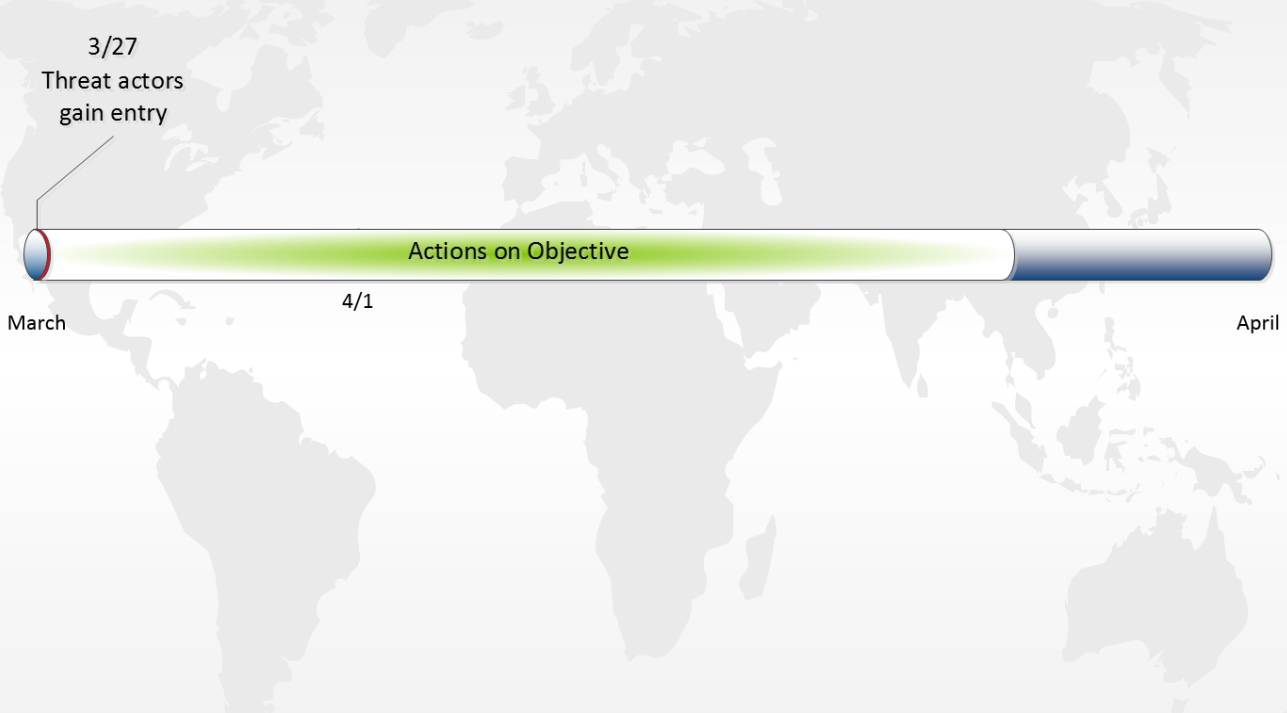
- Ad Hoc – playing whack-a-mole
- Containment – restricting assets or access points
- Compartmented – remediating segments
- Failover – implementing disaster recovery plan
- Full Scope – hunting for access points

Ad Hoc Eviction



Ad Hoc Eviction

TG-1588

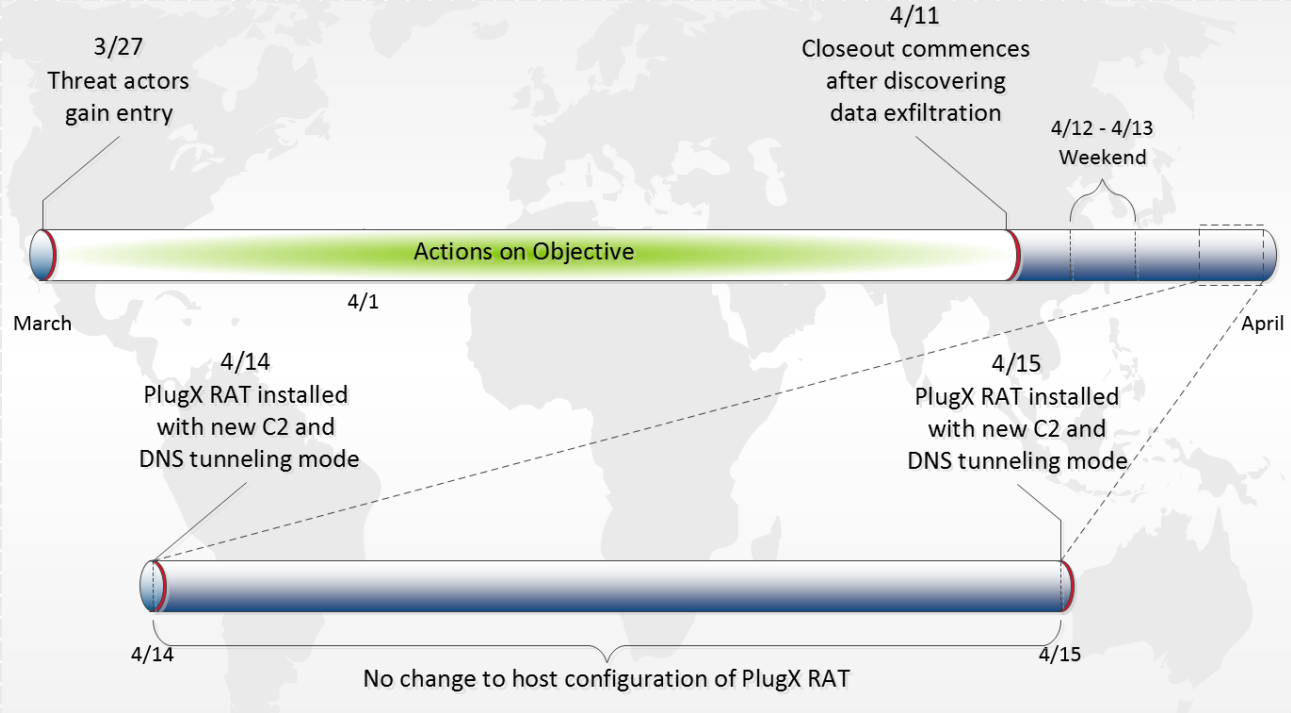


Ad Hoc Eviction

TG-1588

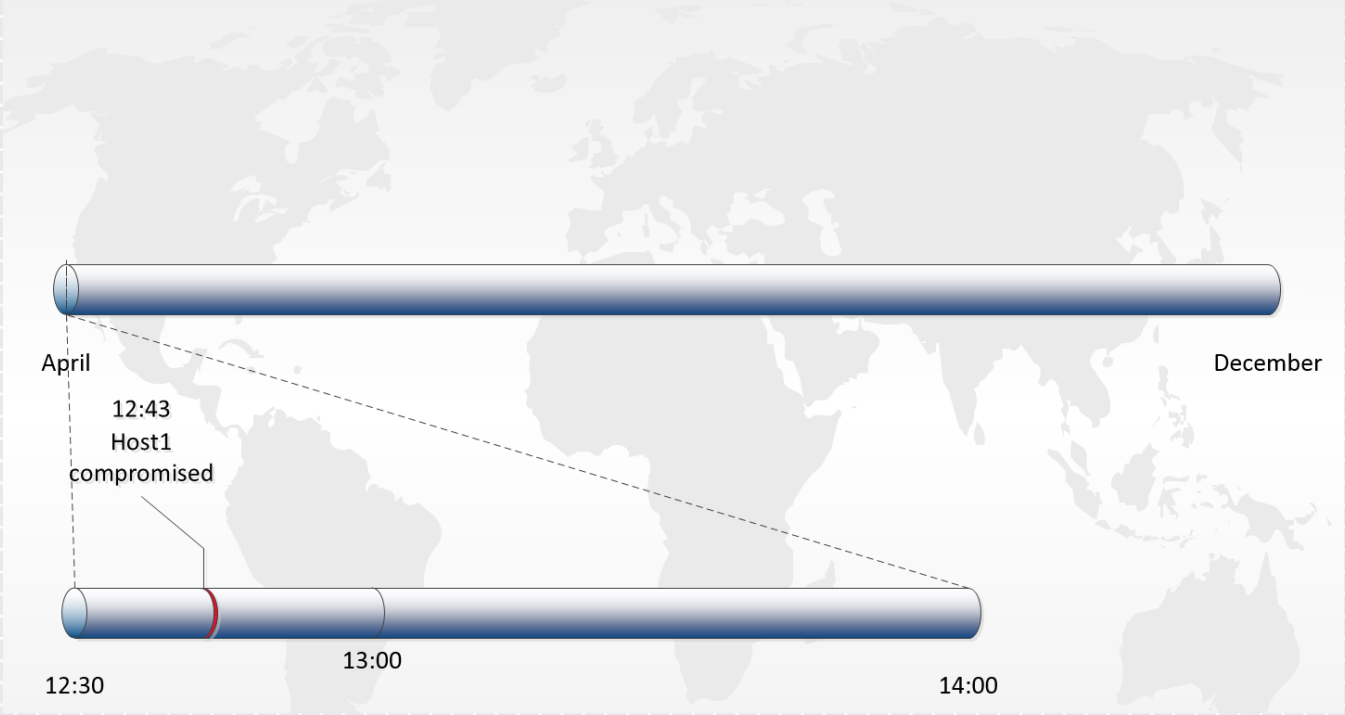
Ad Hoc Eviction

TG-1588



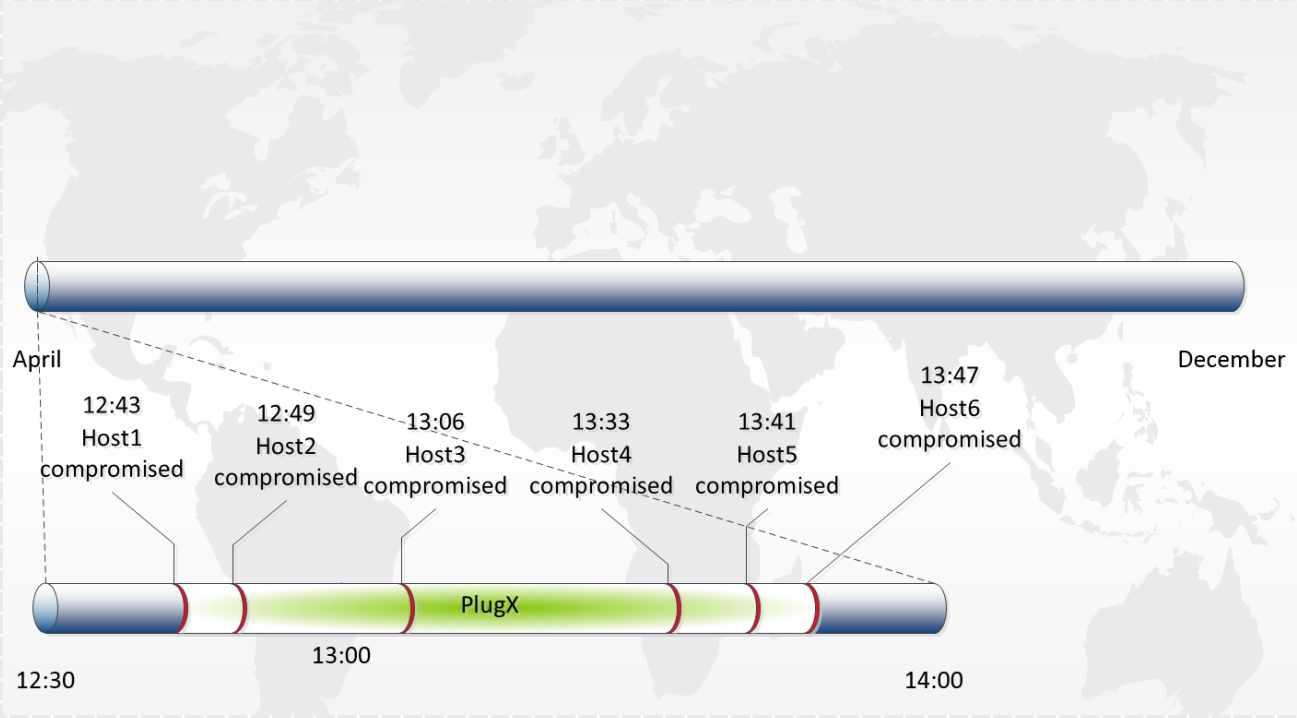
Ad Hoc Eviction

TG-3390



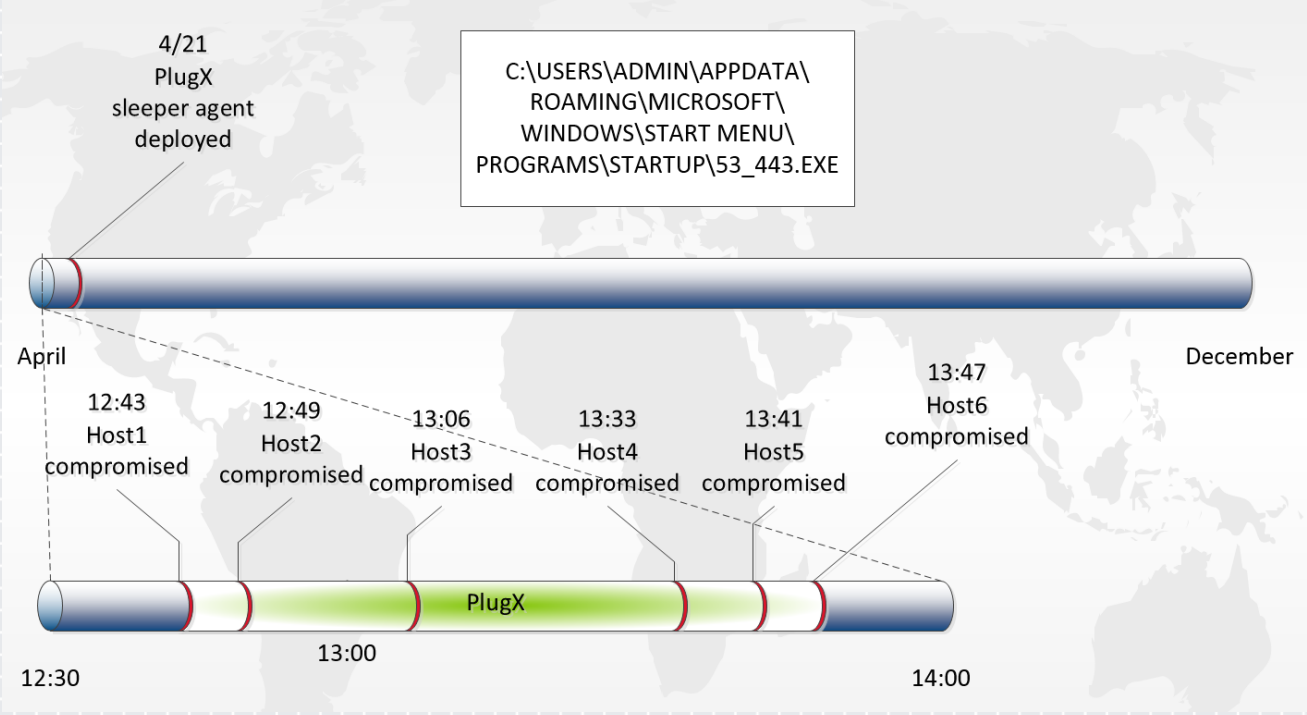
Ad Hoc Eviction

TG-3390



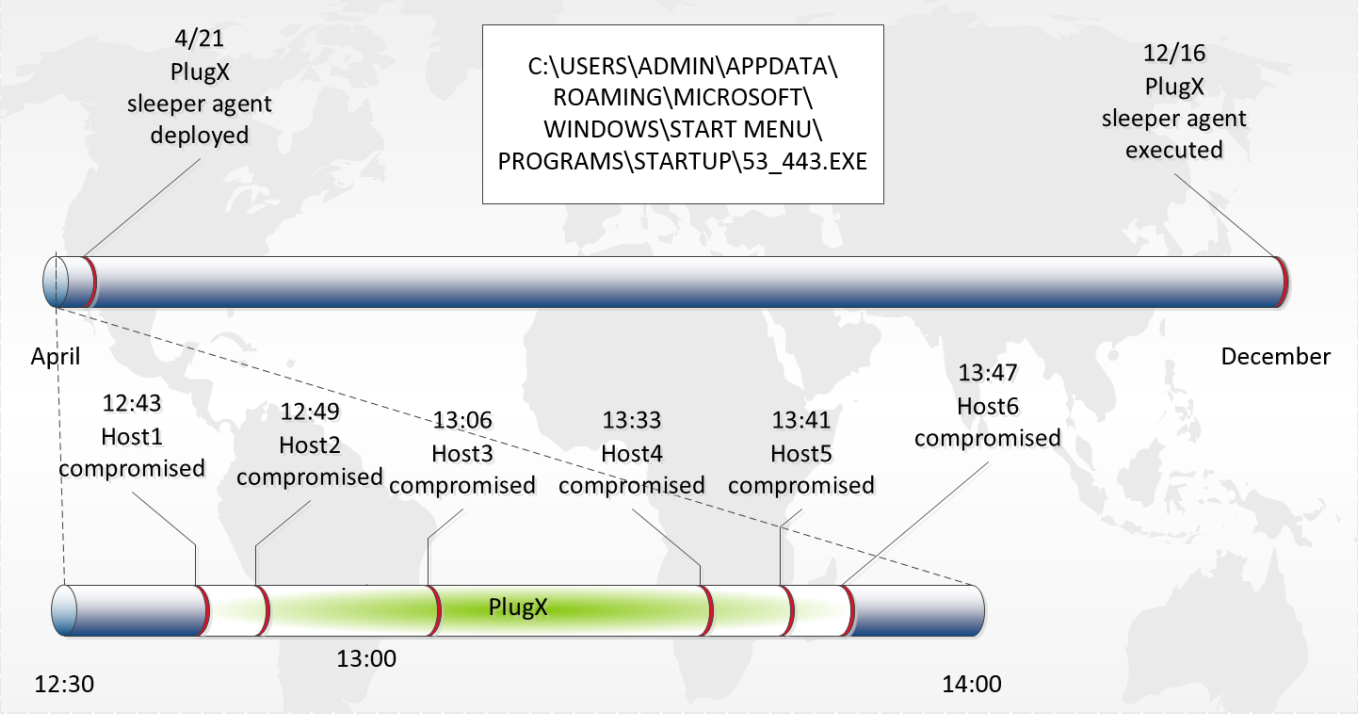
Ad Hoc Eviction

TG-3390



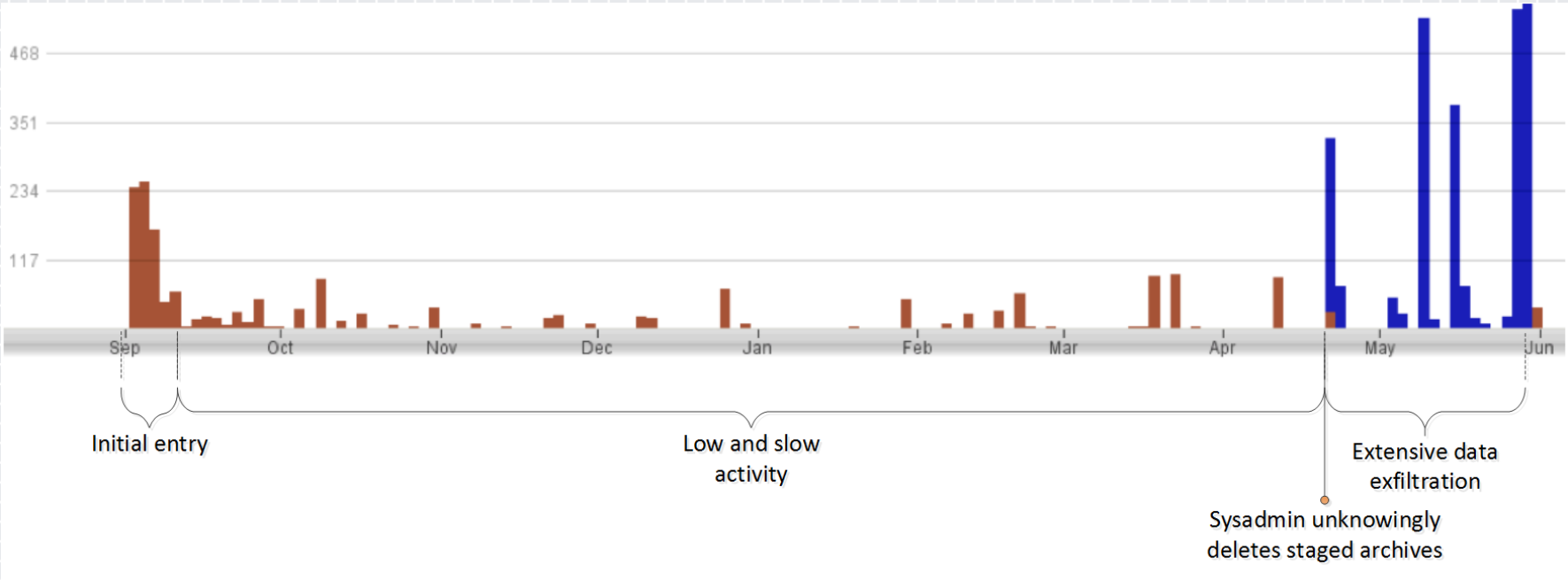
Ad Hoc Eviction

TG-3390

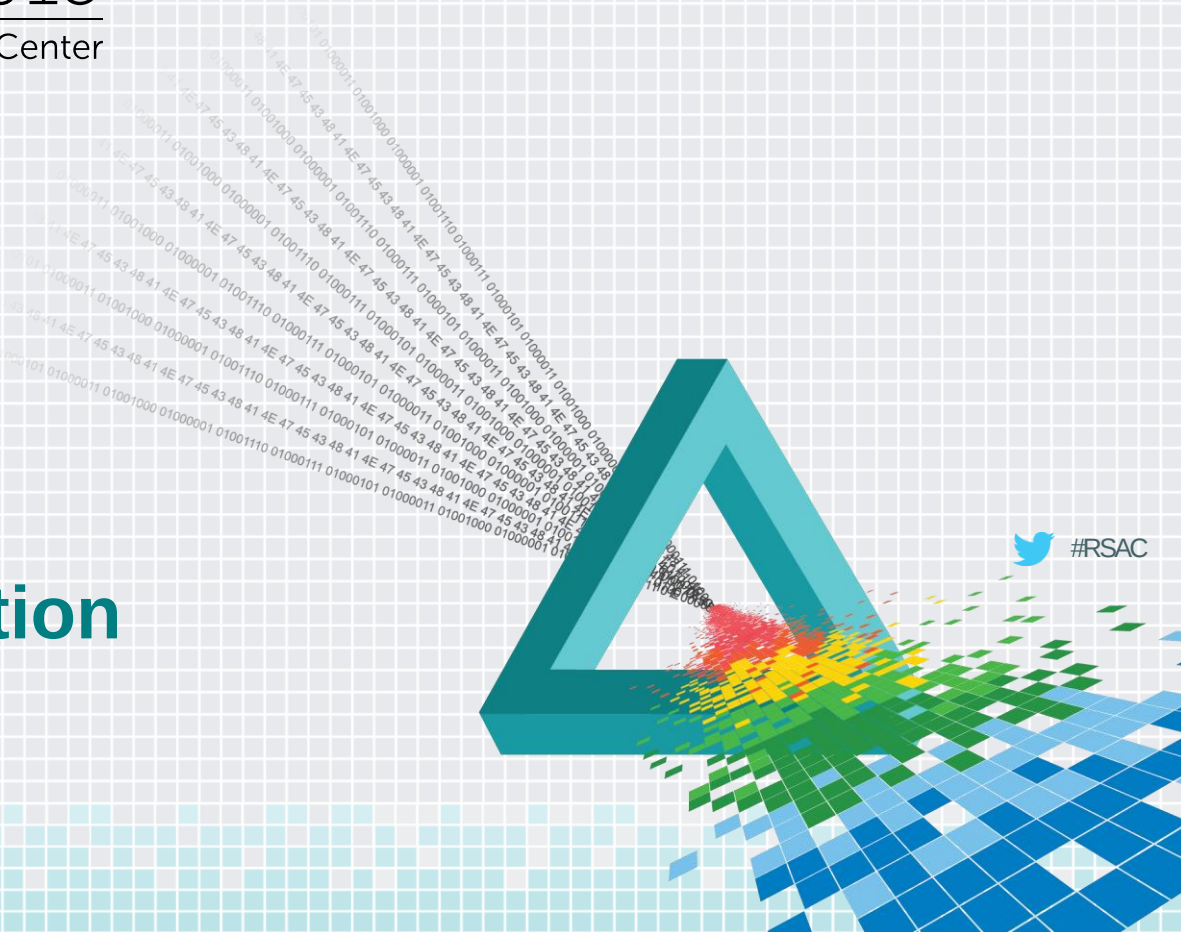


Ad Hoc Eviction

TG-3301

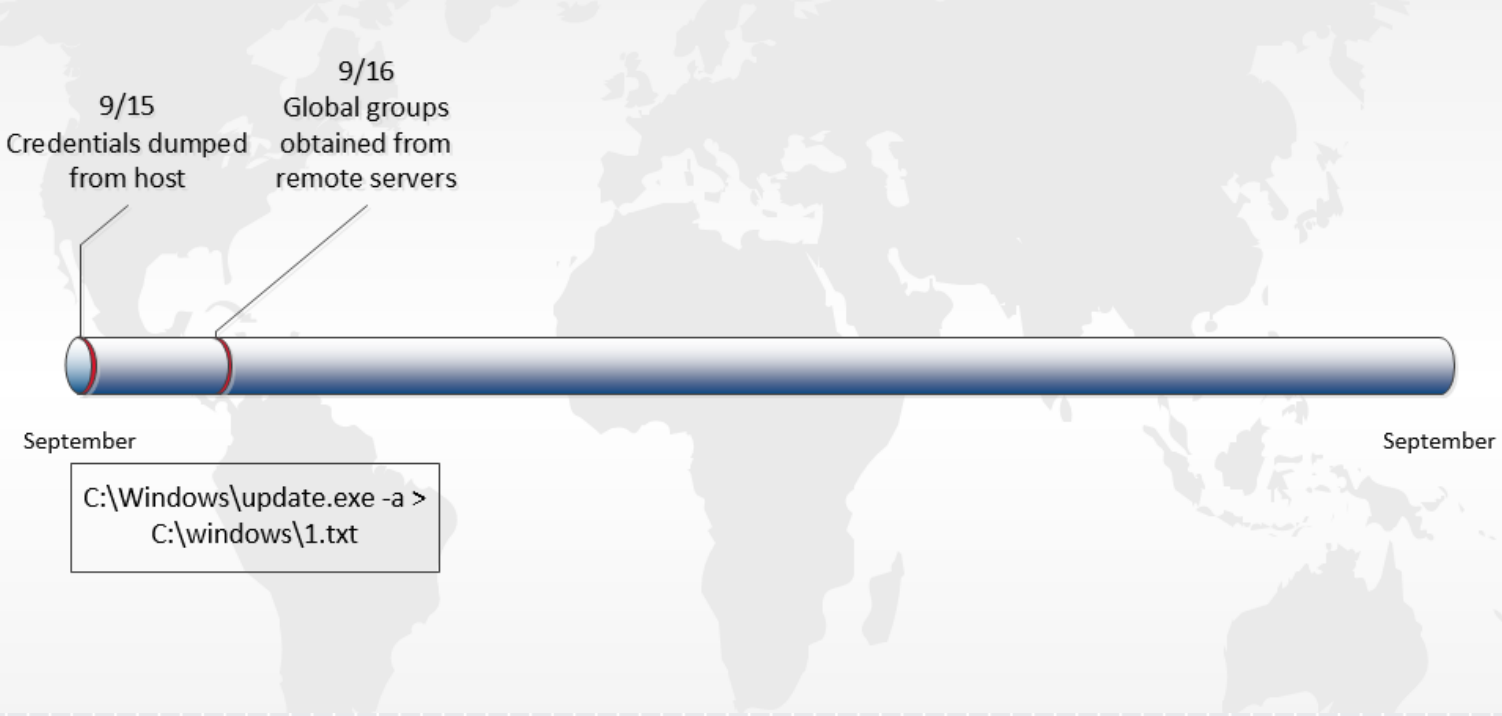


Containment Eviction



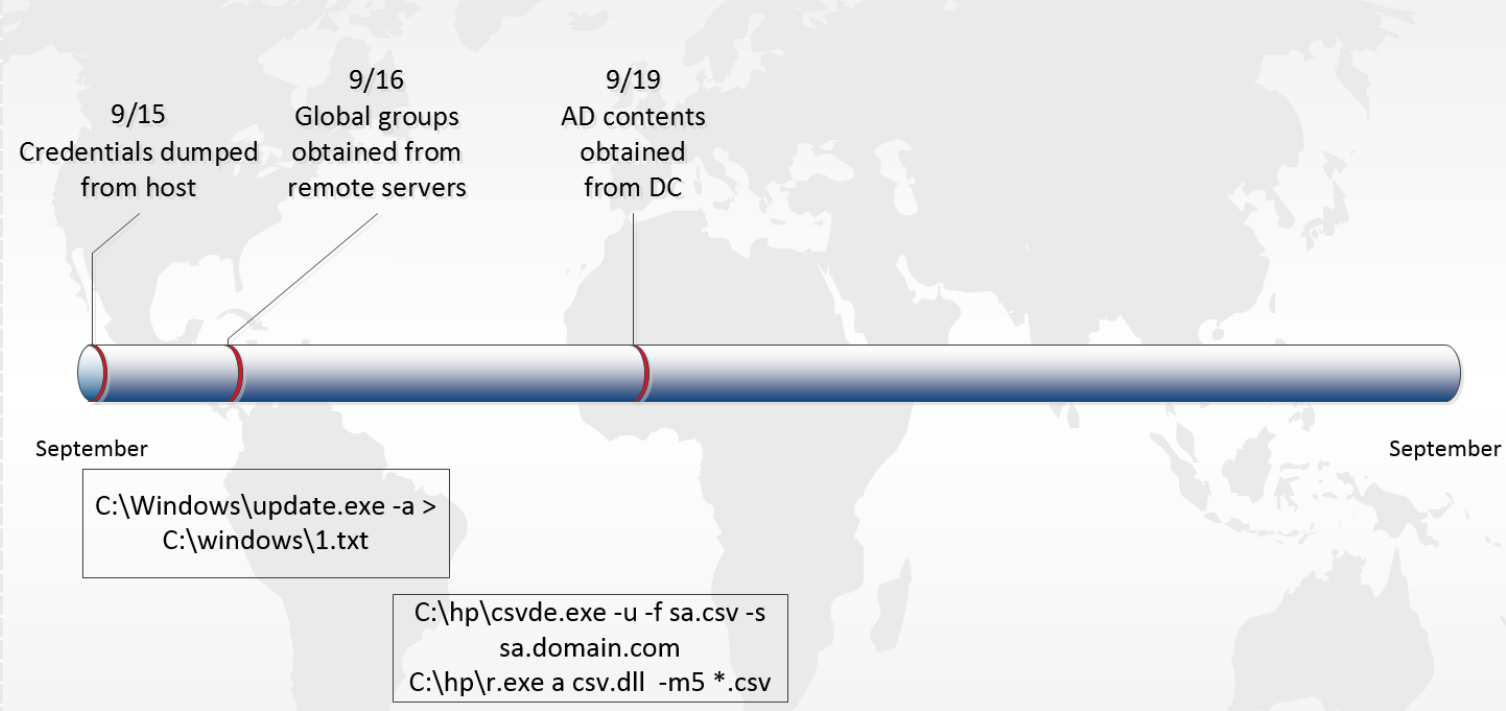
Containment Eviction

TG-0416



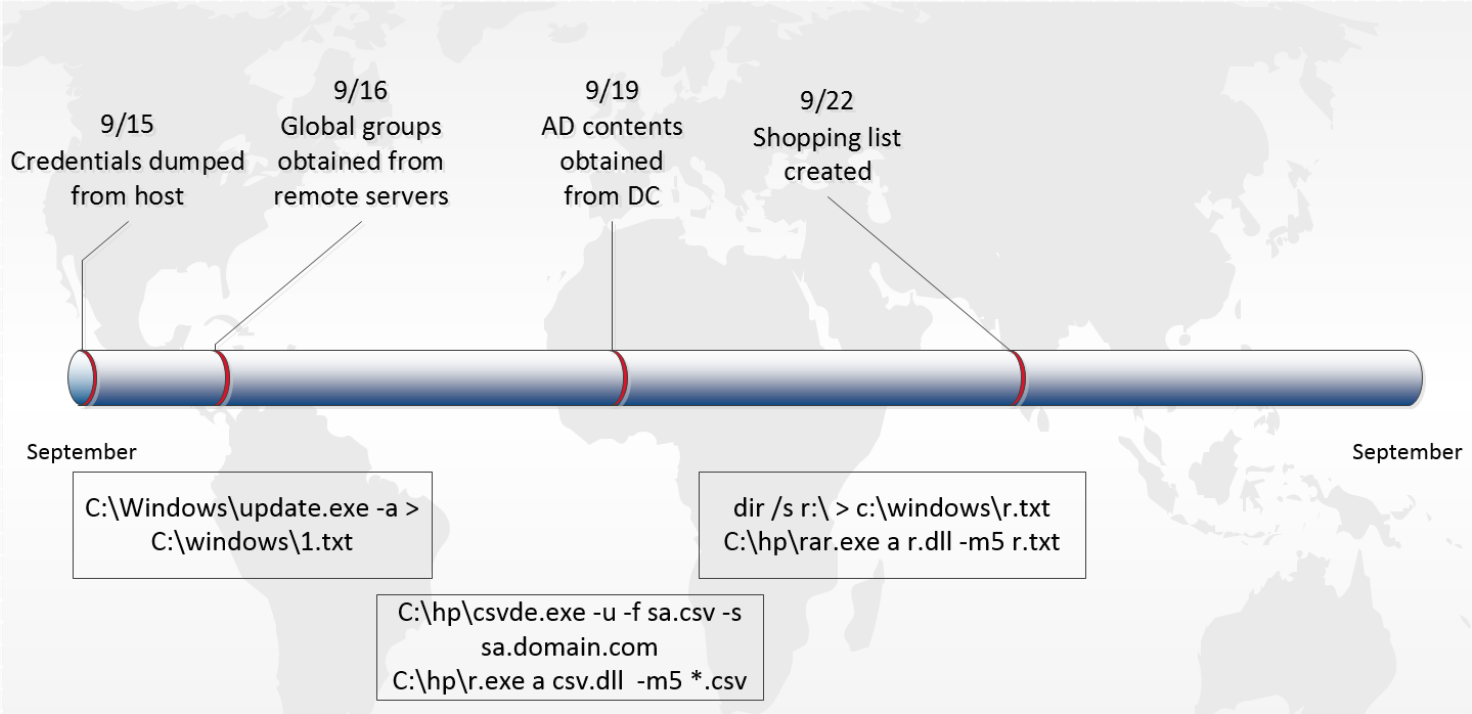
Containment Eviction

TG-0416



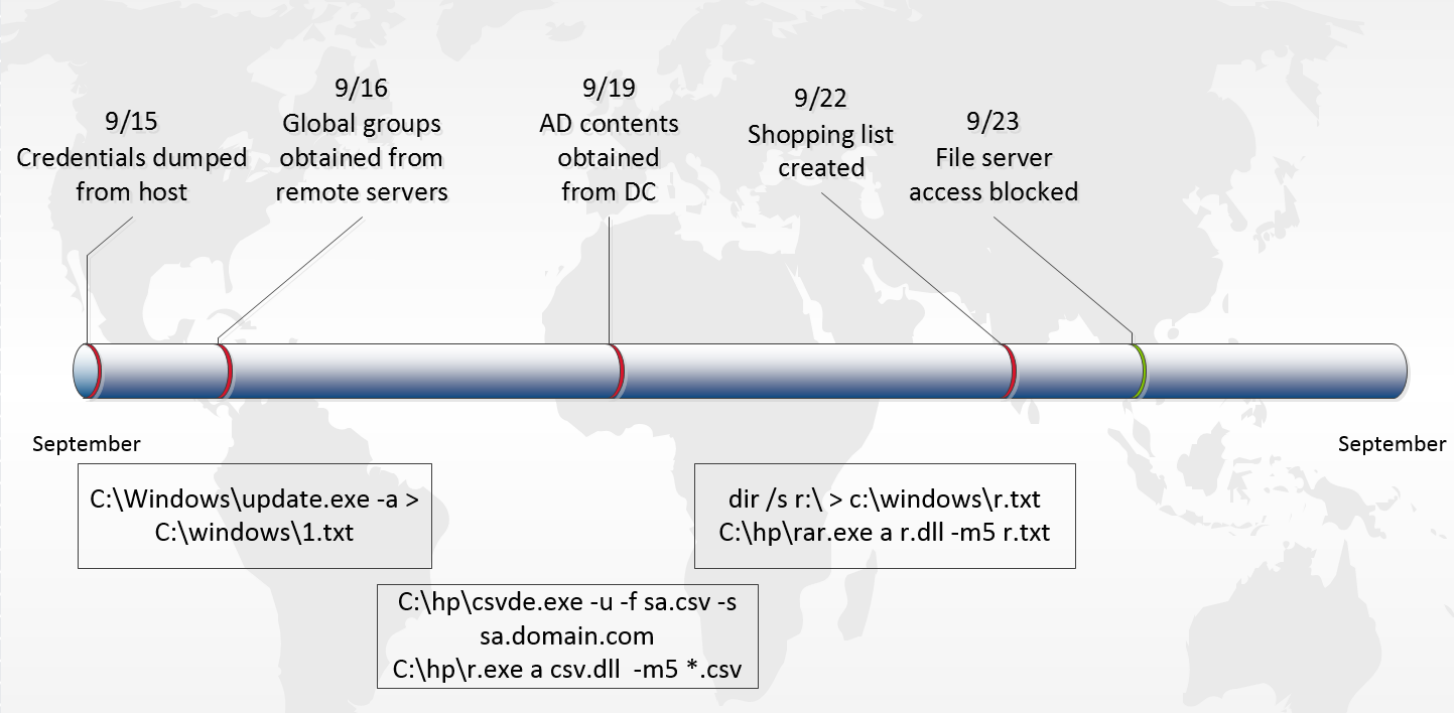
Containment Eviction

TG-0416



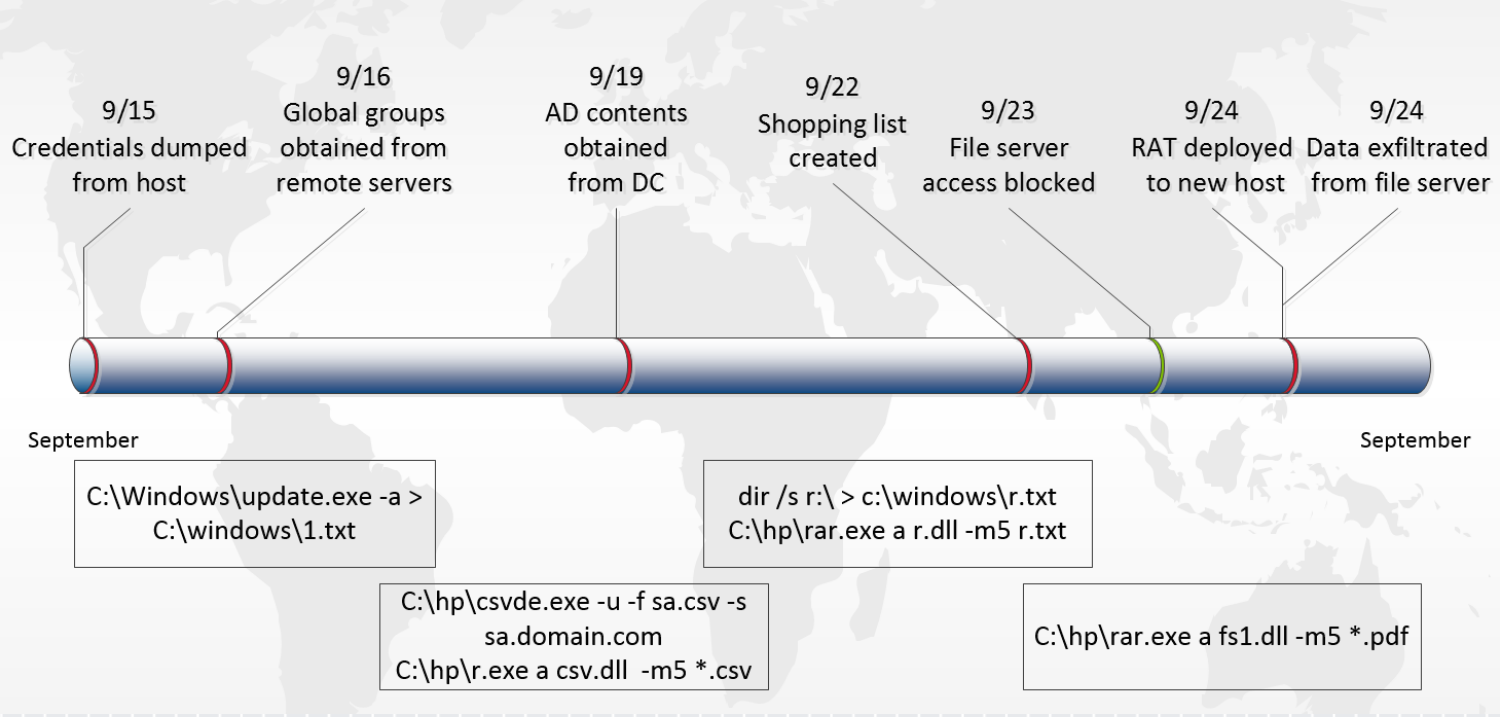
Containment Eviction

TG-0416

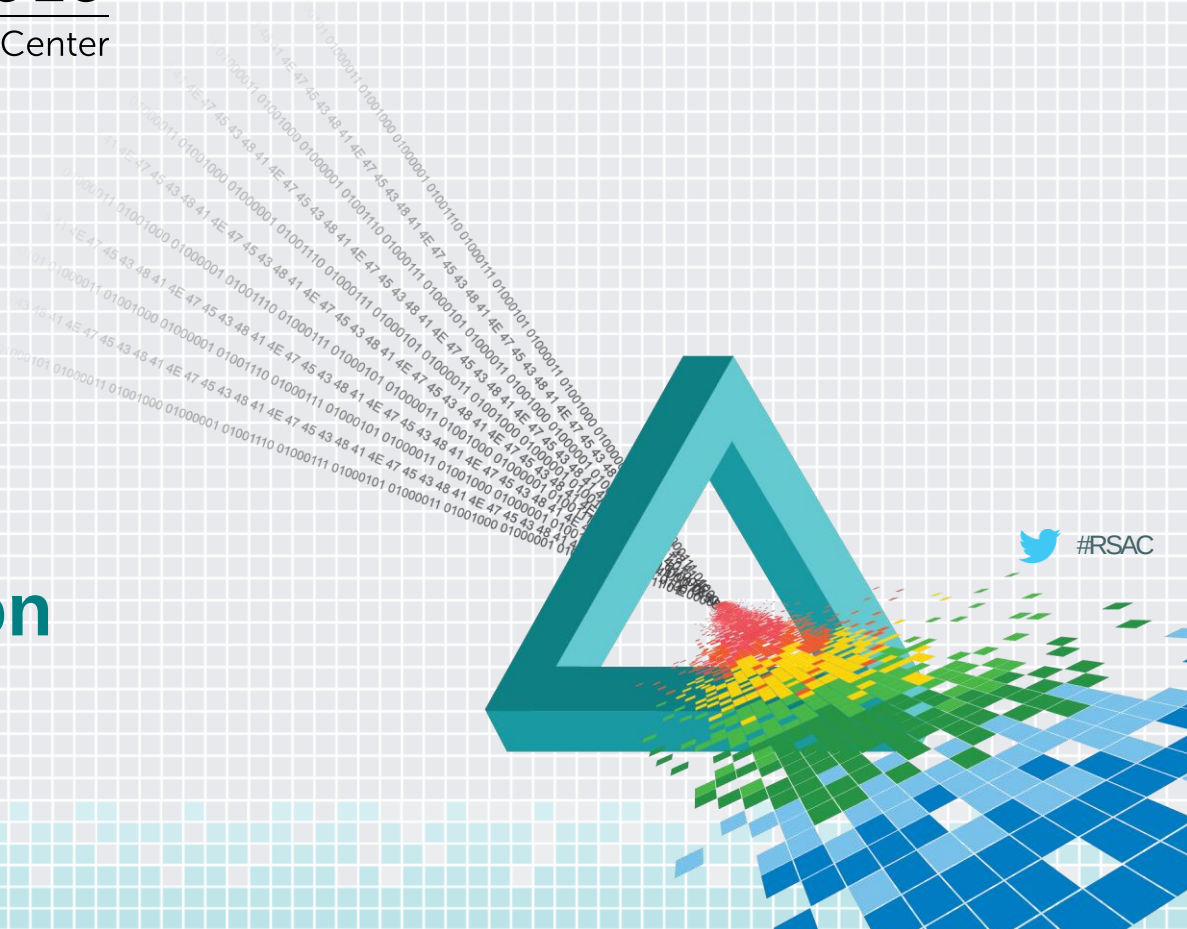


Containment Eviction

TG-0416

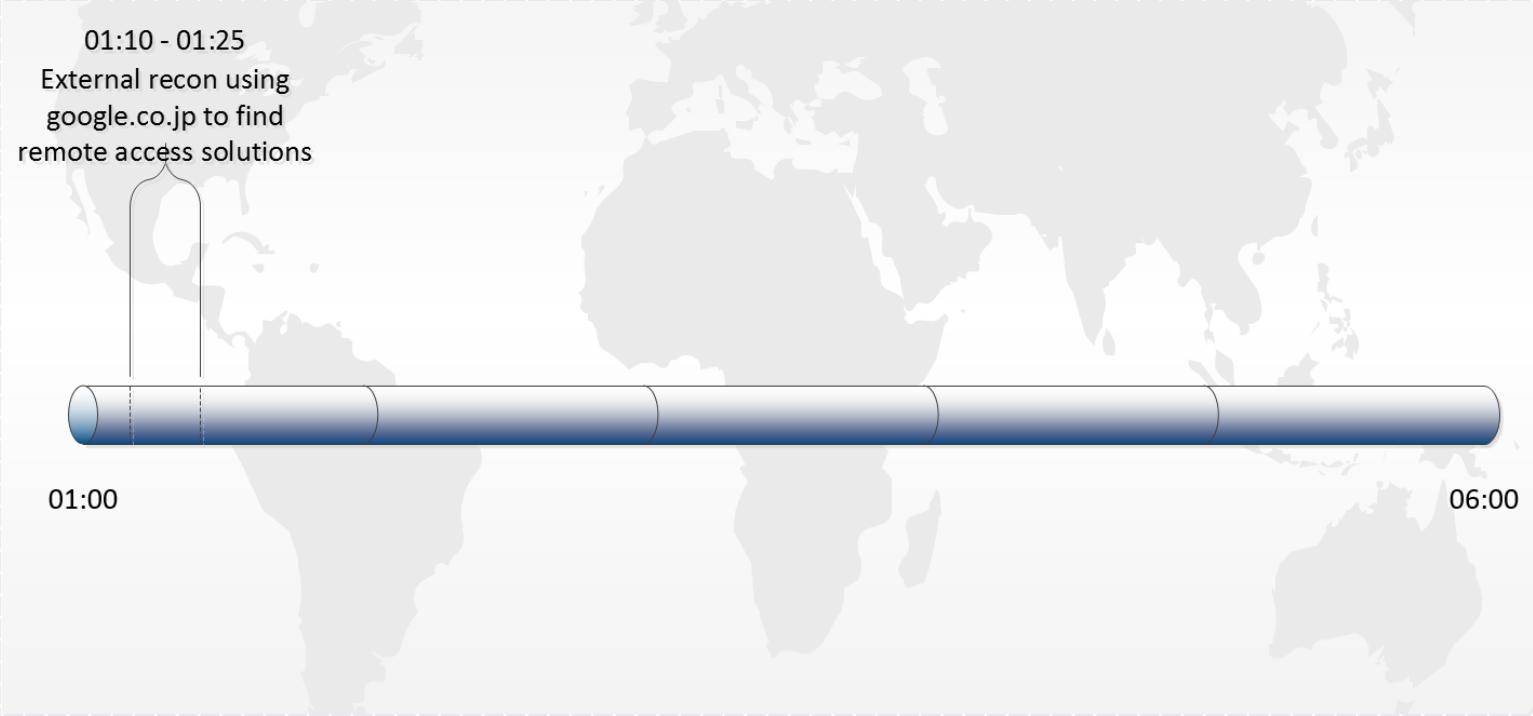


Full-Scope Eviction



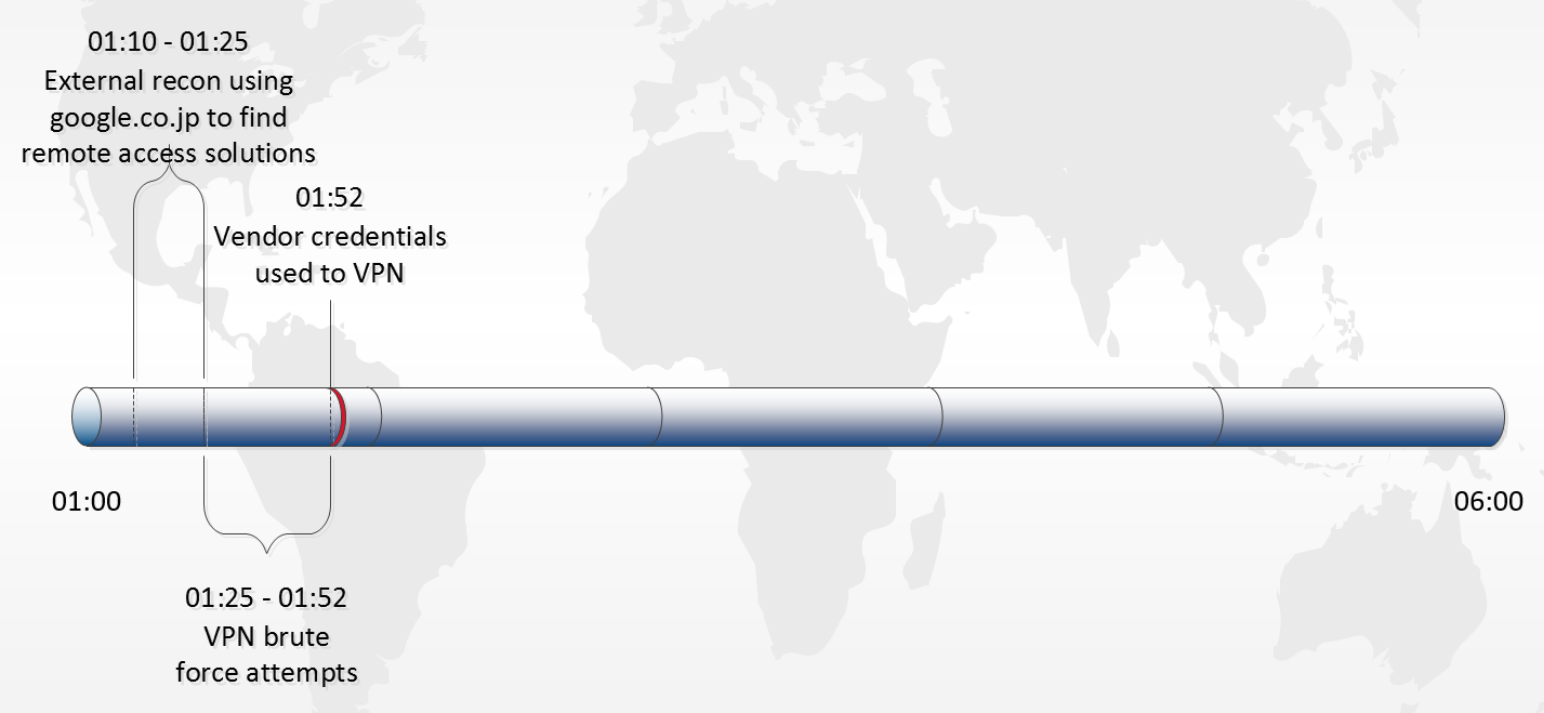
Full-Scope Eviction

TG-3390



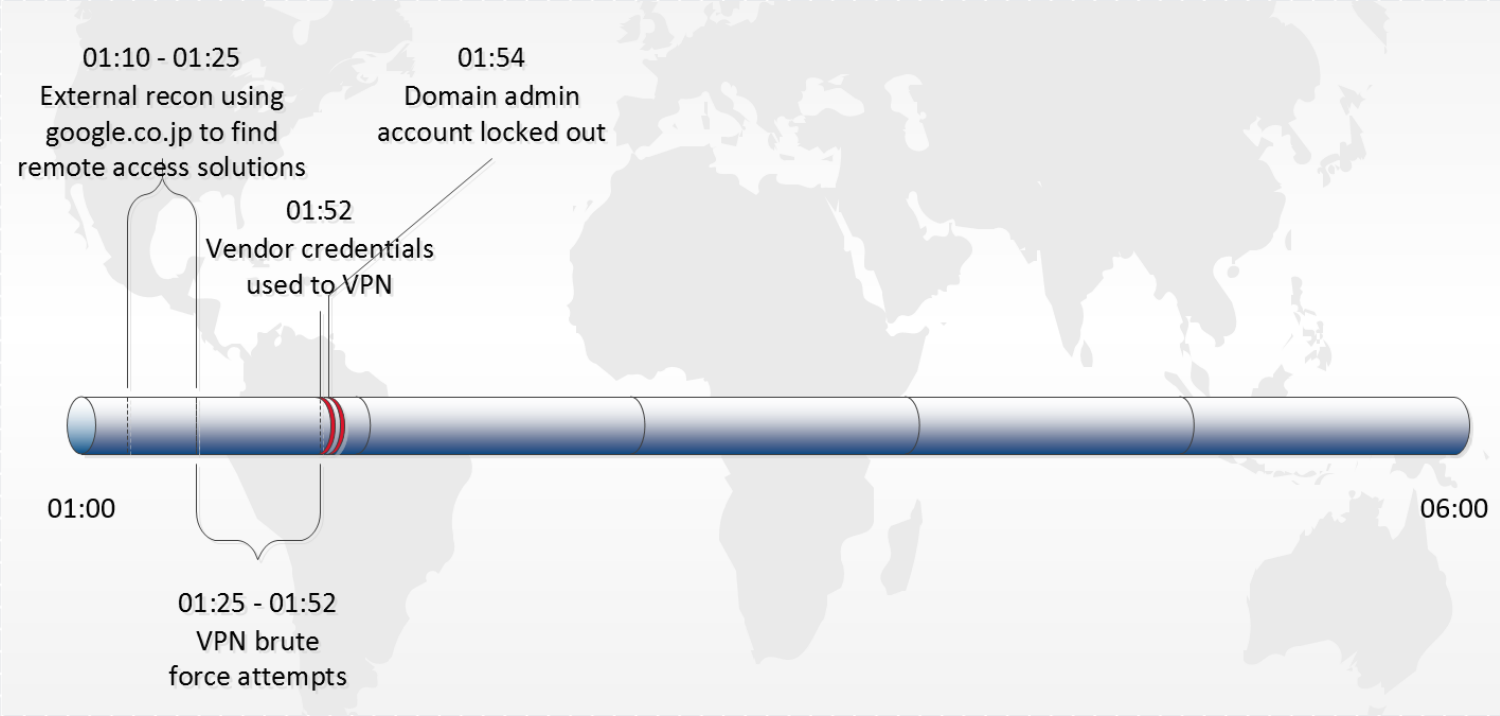
Full-Scope Eviction

TG-3390



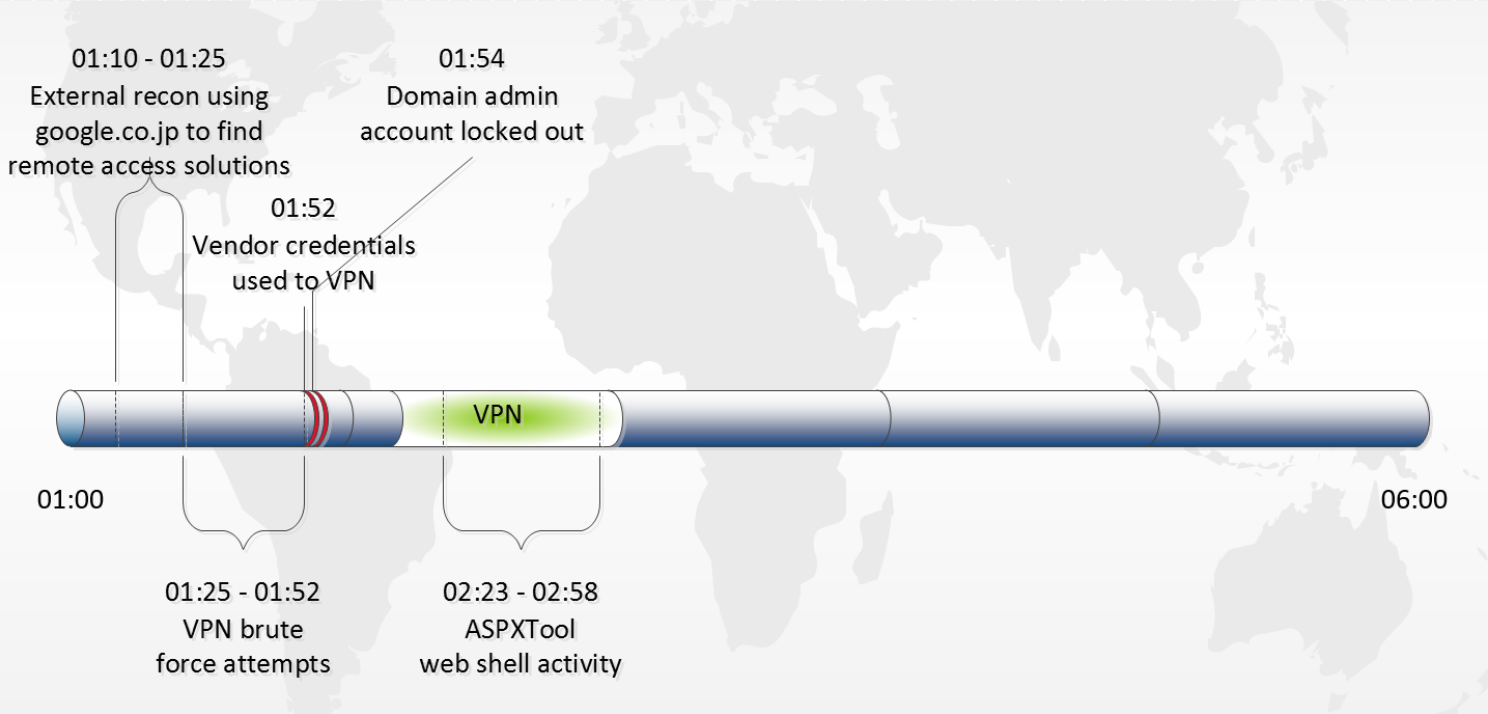
Full-Scope Eviction

TG-3390



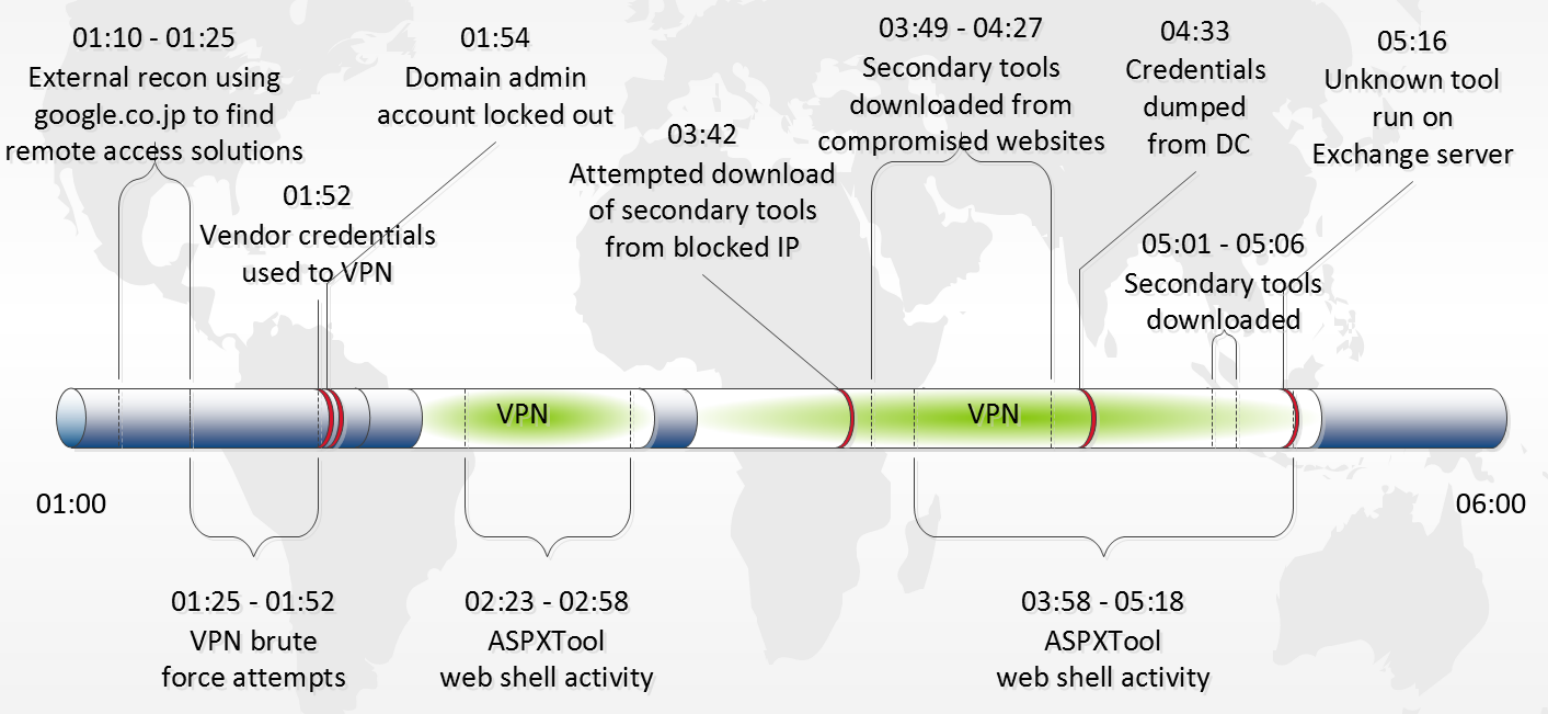
Full-Scope Eviction

TG-3390



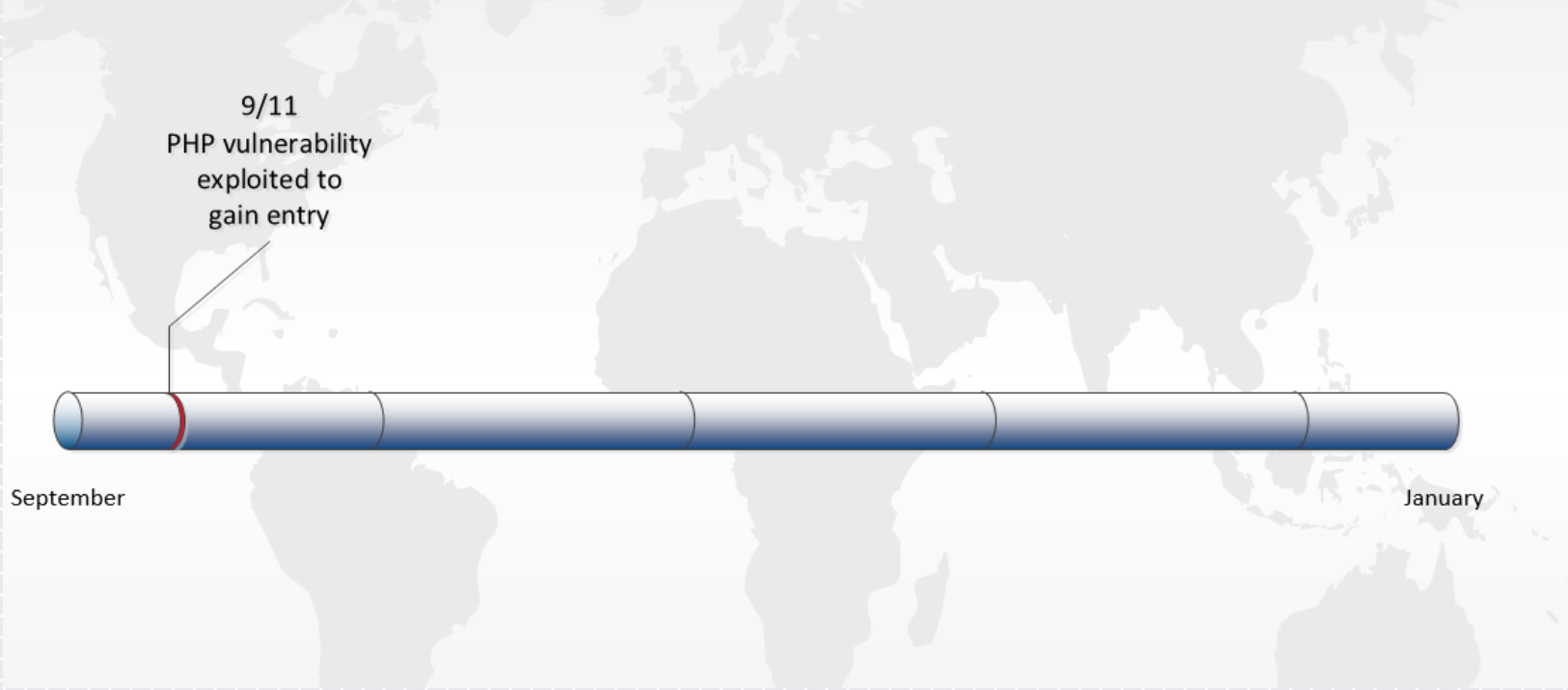
Full-Scope Eviction

TG-3390



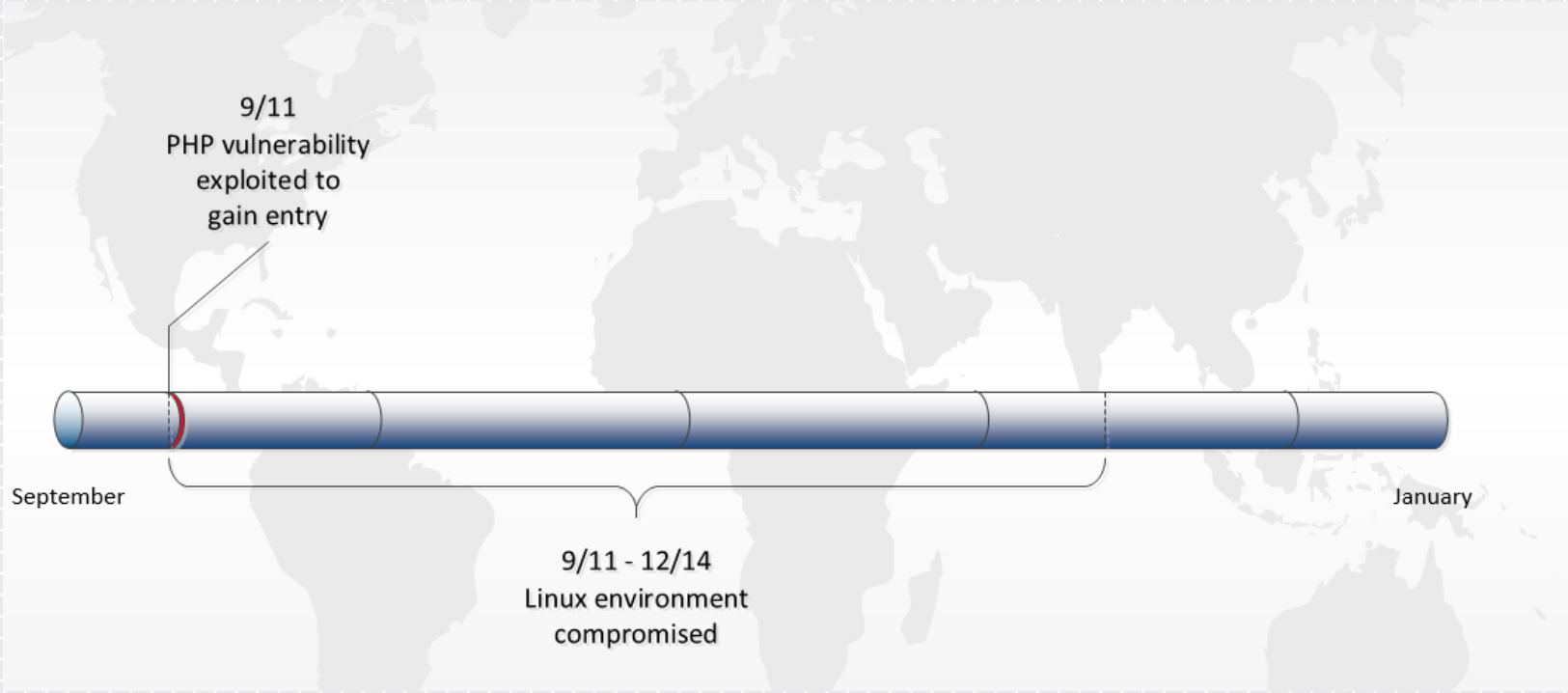
Full-Scope Eviction

TG-1314



Full-Scope Eviction

TG-1314



Full-Scope Eviction

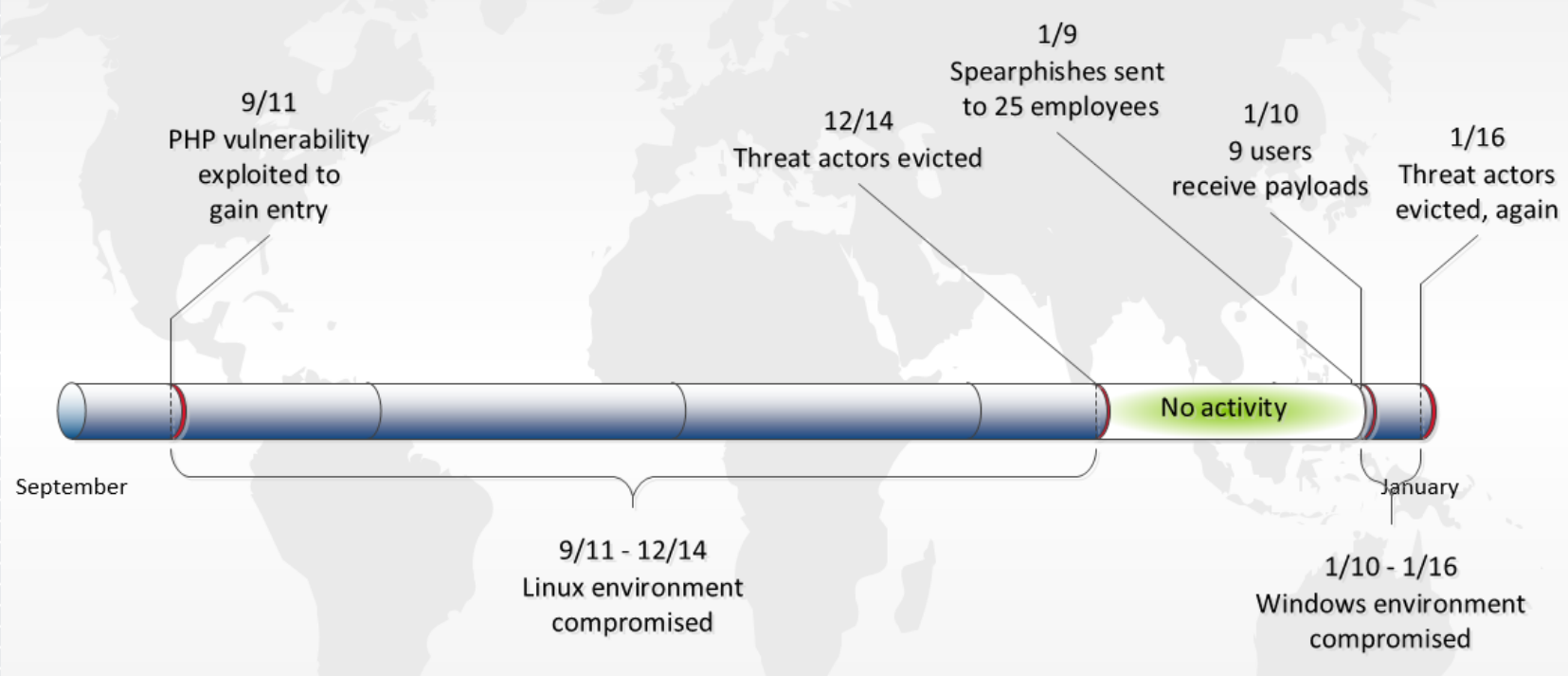
TG-1314

Full-Scope Eviction

TG-1314

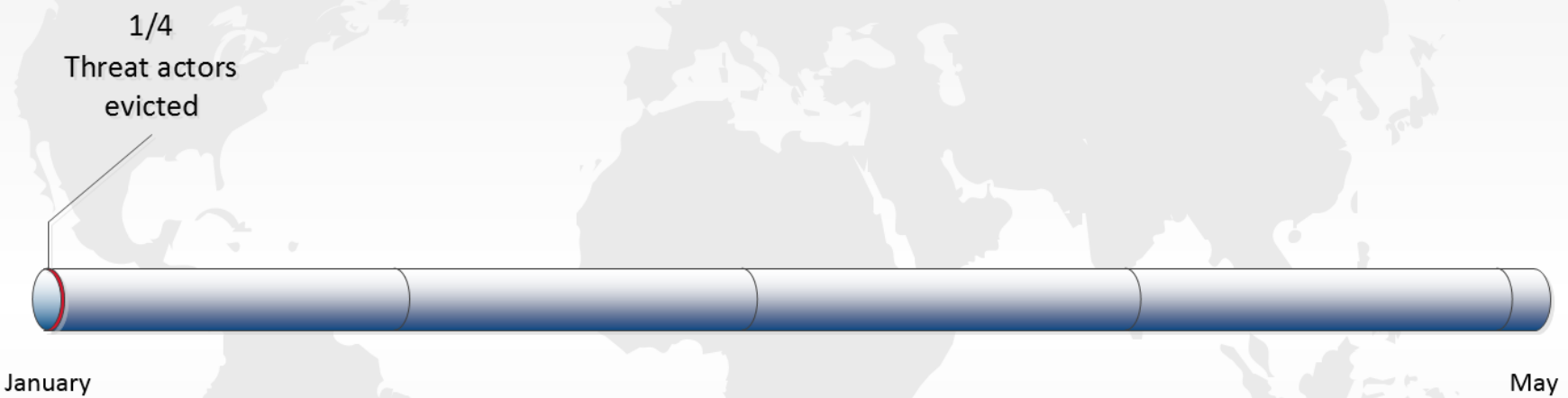
Full-Scope Eviction

TG-1314



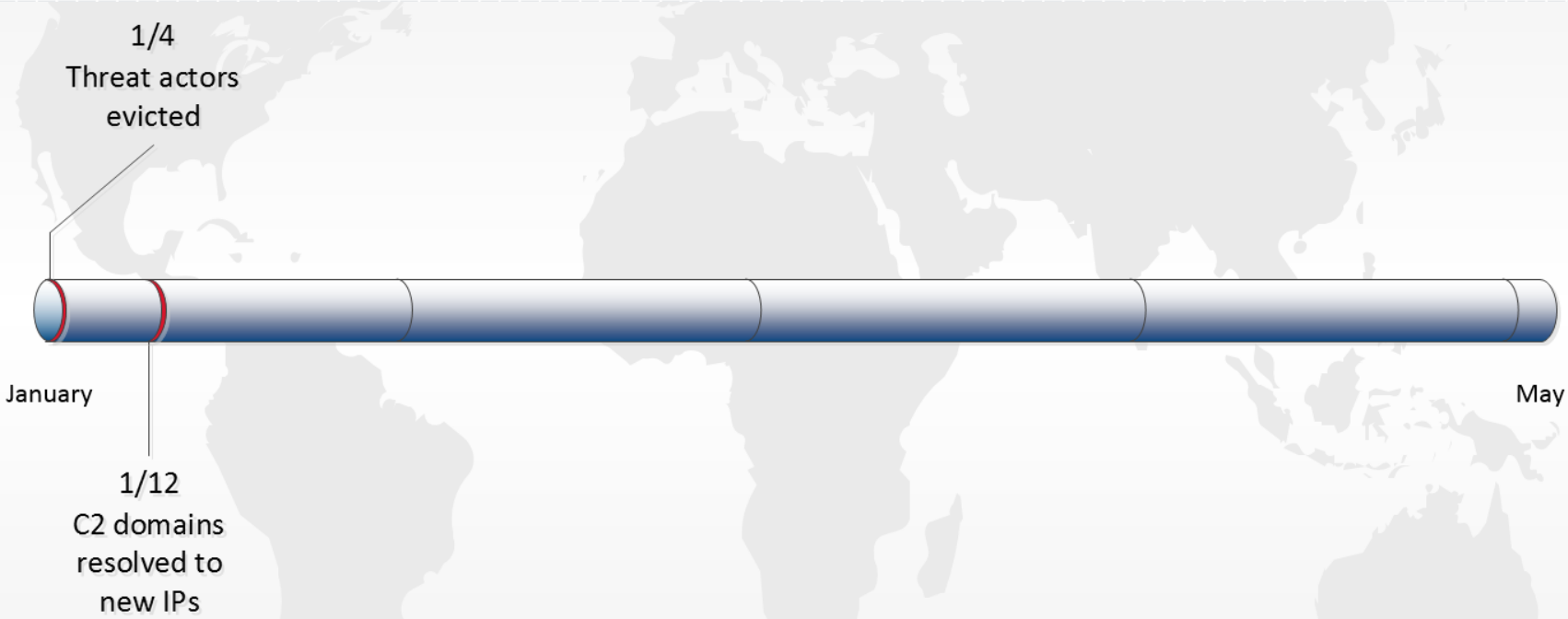
Full-Scope Eviction

TG-1588



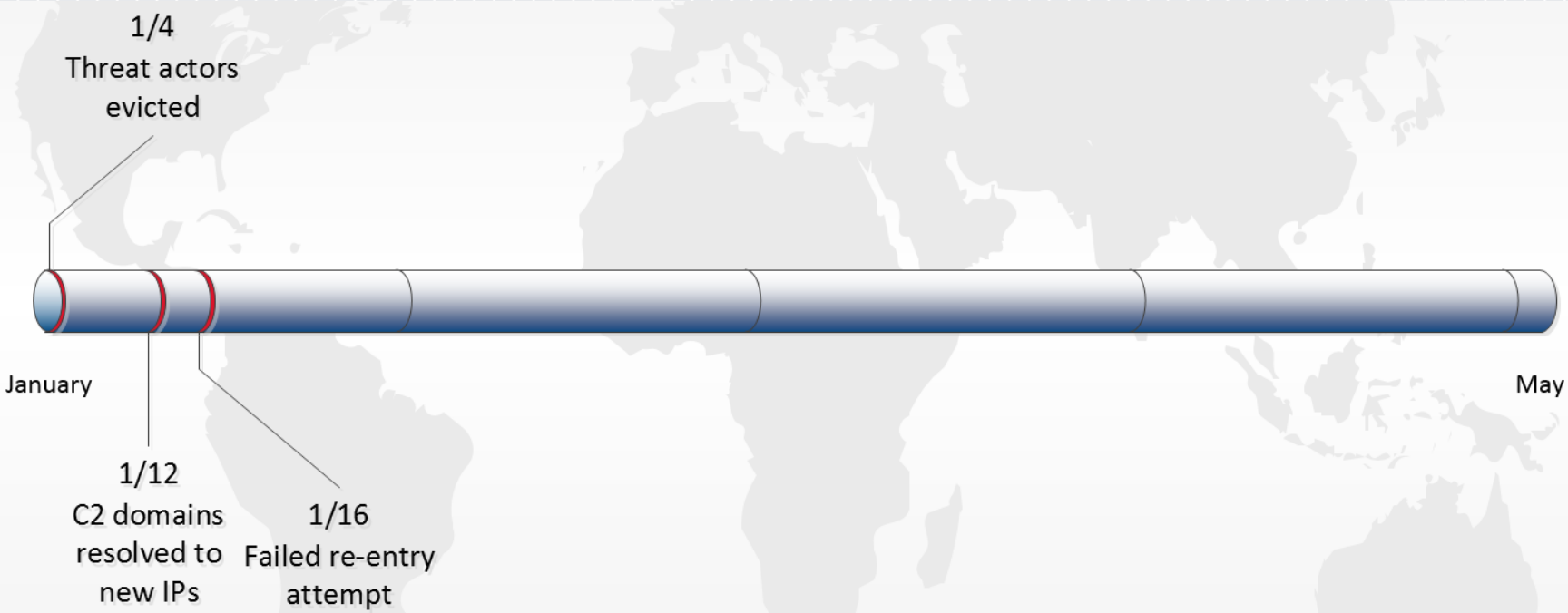
Full-Scope Eviction

TG-1588



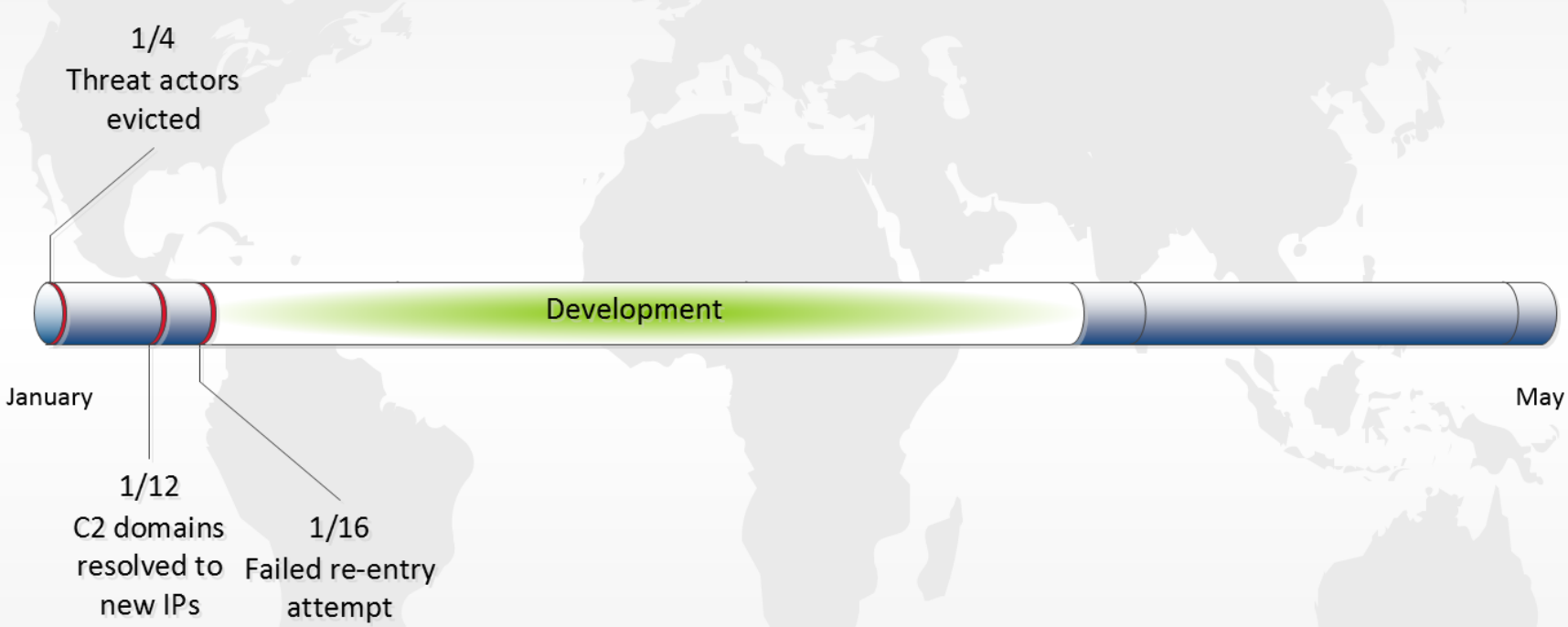
Full-Scope Eviction

TG-1588

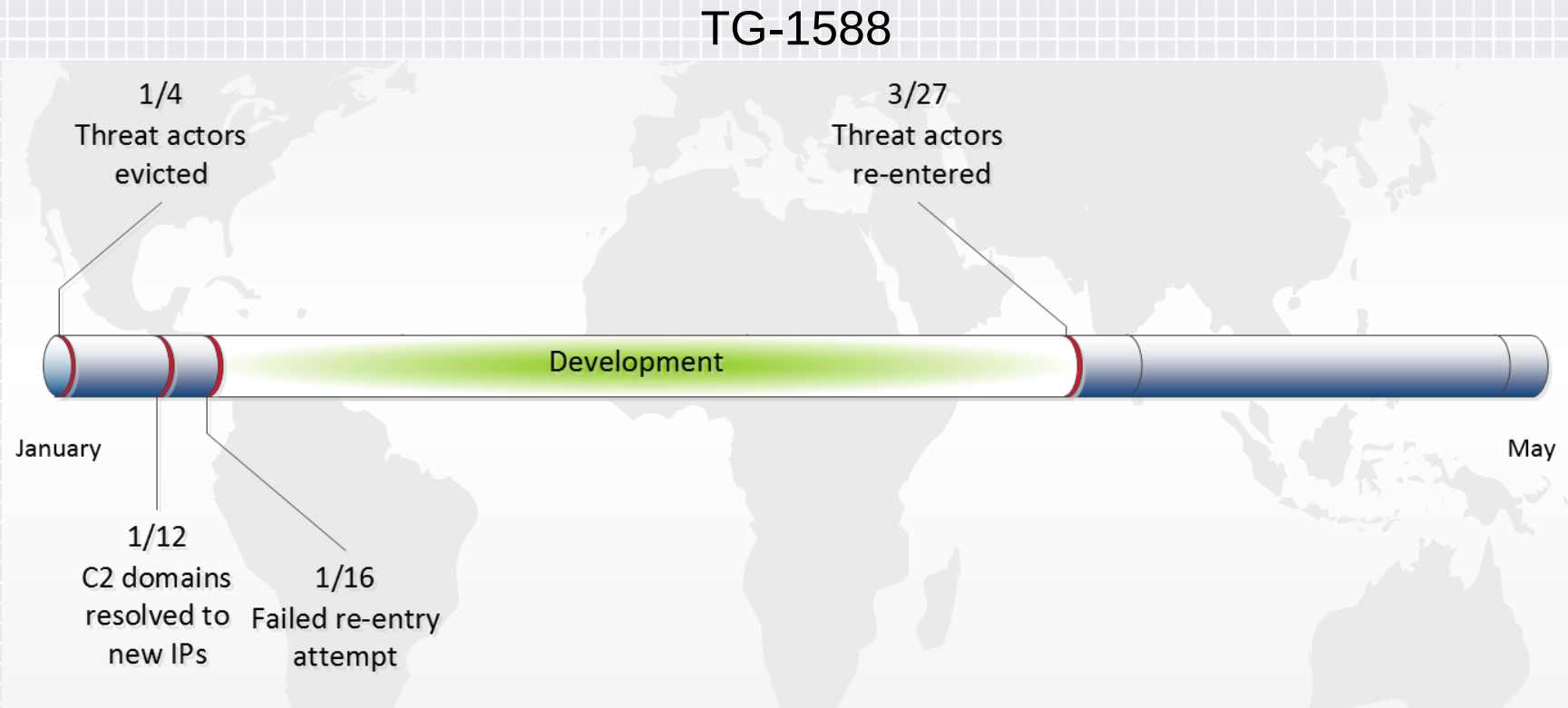


Full-Scope Eviction

TG-1588

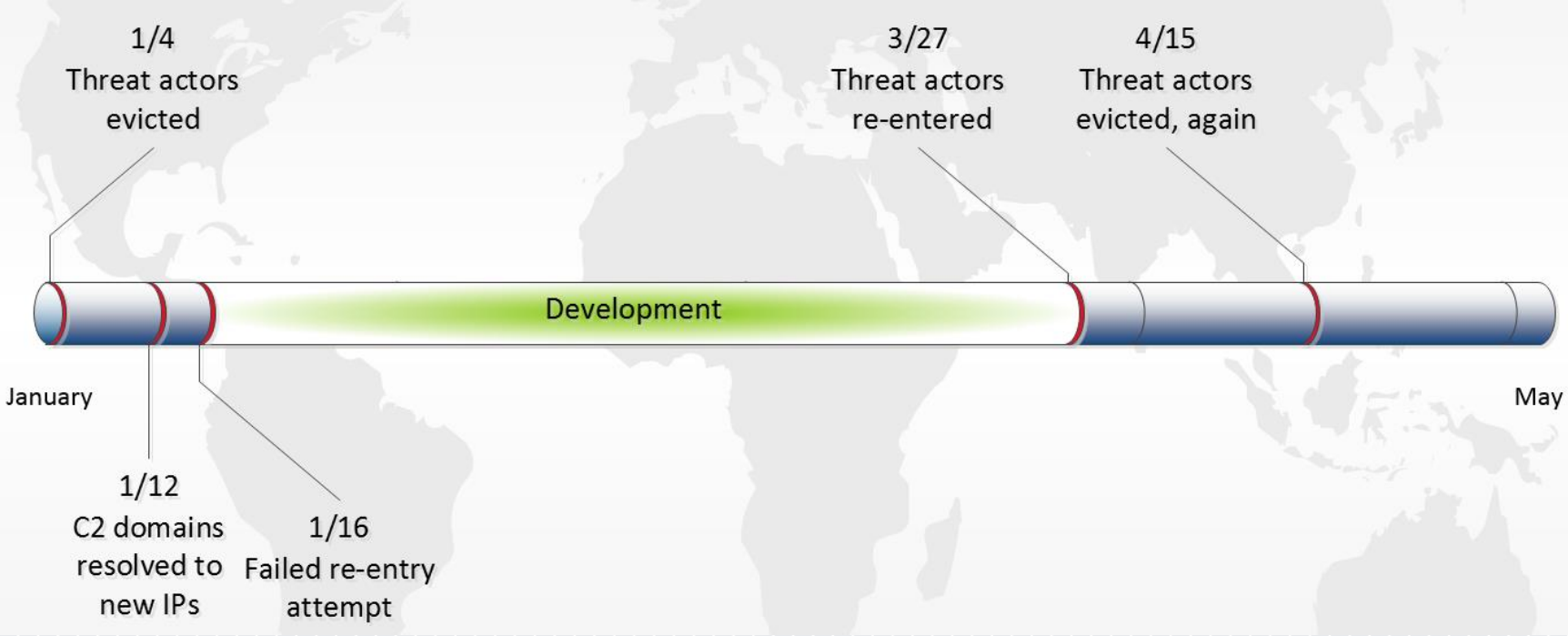


Full-Scope Eviction



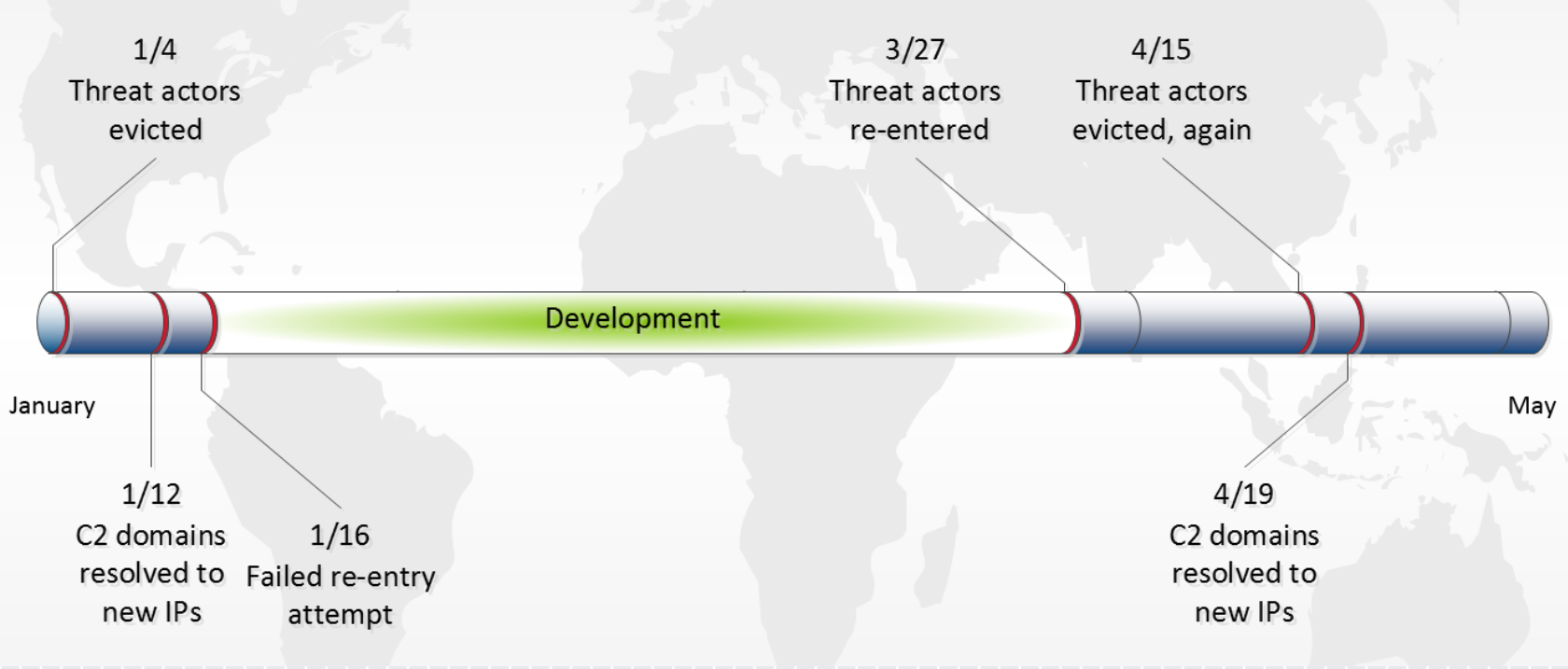
Full-Scope Eviction

TG-1588



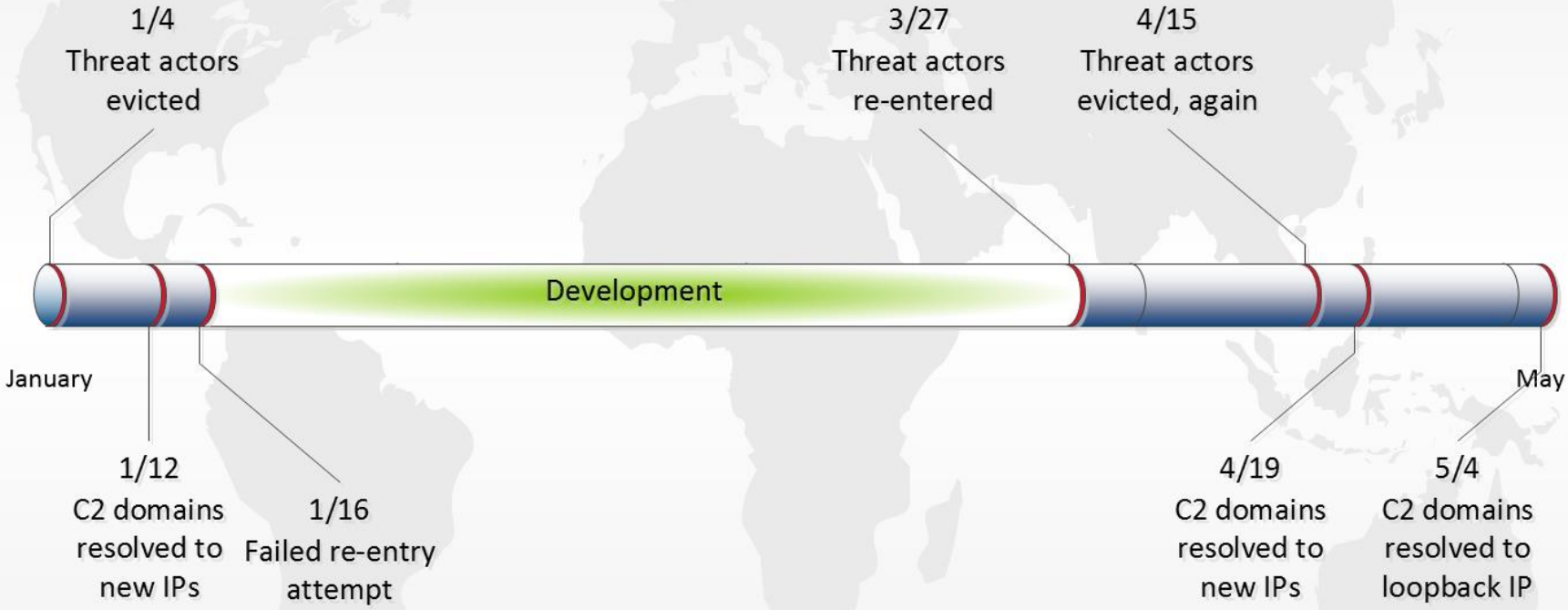
Full-Scope Eviction

TG-1588



Full-Scope Eviction

TG-1588



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

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You