At the 2013 RSA security conference in San Francisco, Dell SecureWorks Counter Threat Unit™ (CTU) researchers will present some new techniques we have found around sinkholing. We believe these techniques will assist security researchers in their work.

Sinkholing gives researchers a unique perspective on past, present and future attacks. At times, the CTU research team re-animates infected systems that have been inactive for months and finds victims who have remained infected despite ever-improving antivirus protections. The CTU research team sometimes takes control of domains that are being used for both ongoing attacks and for development of new types of malware, and then leverages that intelligence to protect organizations before they become victims.

For example, CTU researchers have successfully taken over a set of domains related to the RegSubsDat and Enfal malware families, enabling us to disrupt the threat actors' communications to their botnet and notify the victims. The CTU research team publicly released these findings in the reports The Sin Digoo Affair and The Mirage Campaign.

We have used this tactic to take down multiple botnets related to targeted attacks and alert numerous victims to the presence of Advanced Persistent Threat (APT) malware on their networks. Through this activity, we have been able to leverage the collected intelligence to proactively develop defenses for our customers for malware threats that were previously unknown to antivirus vendors and to the security community.

Deep Analysis of Sinkholes Help Identify Targets and Malware

The CTU research team implements sinkholes to gain a deeper understanding of the targets and types of malware used by threat actors. The primary objective of our sinkholing operations is to answer the following questions:

- Who are the infected victims?
  - Why are they a target?
- What malware types are we seeing from the victims?
- What do we not already know about this domain?

Simply knowing someone is infected doesn't provide any context about the malware or the threat actors. By analyzing the sinkhole traffic, we can start to understand the 'what and why' behind these victims. If we can link the infected victims to the unique malware that was used, we can form a larger picture of the groups behind the attack (see Figure 1).

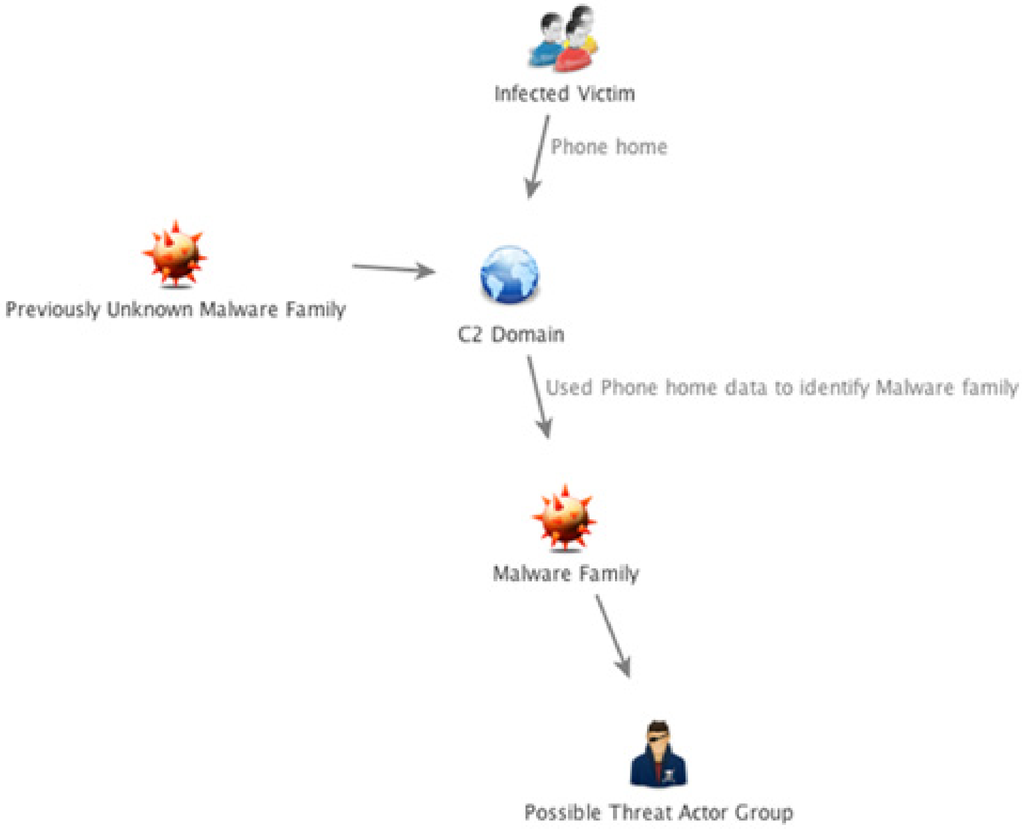

Infected Victim
Phone home
Previously Unknown Malware Family
C2 Domain
Used Phone home data to identify Malware family
Malware Family
Possible Threat Actor Group

Figure 1. Digging deeper into our collected data can help us understand who is behind these attacks. (Source: Dell SecureWorks)

Threat actors often share or reuse a domain or multiple subdomains for different types of malware. This information can be extremely important for linking malware families based on the shared infrastructure that attackers control. At times, this technique can also help identify anomalies that may be missed when not doing a packet-level analysis. These anomalies are usually associated with new malware or lesser-known variants that were changed to evade existing security controls. By doing this deep level of analysis, CTU researchers can catch these anomalies and ensure that we have defenses in place to protect our customers.

Case Studies

Protux in an International Organization

Protux is one of the oldest malware families associated with APT activity. One of the early reports of its use was an article on targeted spearphishing attacks against Tibetan activists in March 2008. In May 2011, CyberESI analyzed Protux's operational capabilities when it was observed being distributed through a spearphishing campaign with a malicious document titled "Laden's Death.doc". This campaign reportedly targeted U.S. government agencies.

We first encountered Protux in December 2012 while researching the possible targets of another malware family. While analyzing samples from public reports, we identified three unregistered command and control (C2) server domains. After registering the domains, we determined that the only active victims phoning home were using the Protux malware.

Sinkholing the domains revealed almost 300 infected hosts that were phoning home to two of the domains. The only way to thoroughly analyze the hosts was to decode the phone-home requests, which contained the infected system's name, and attempt to attribute the names to either companies or individuals.

We concluded that the two domains with a high count of infected victims were probably not related to APT activity. The majority of the infected hosts we saw were phoning home from residential Internet service providers, primarily in India (see Figure 2).

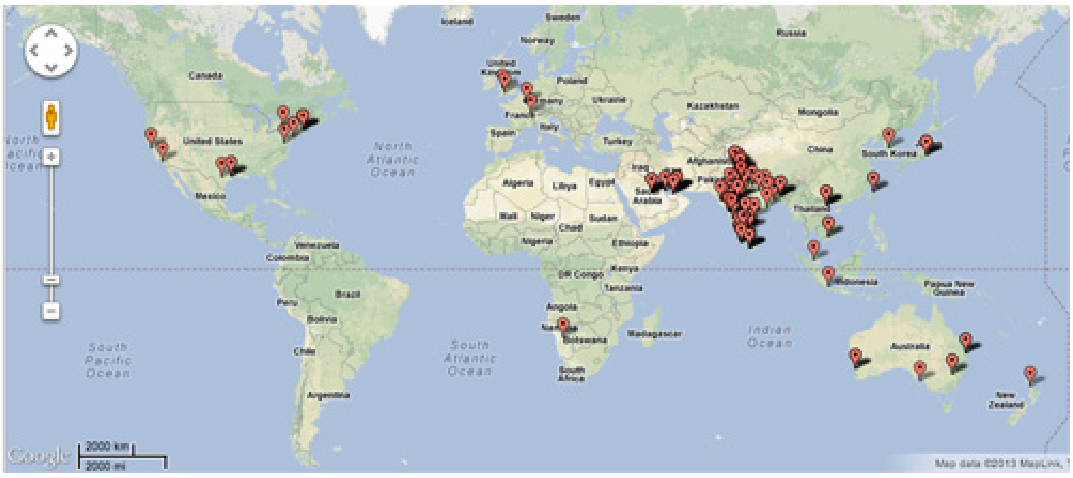


Figure 2. Infected hosts related to Protux. (Source: Dell SecureWorks)

We sometimes find that smaller hacking groups use the same tools and malware but are not affiliated with the primary hacker groups that have espionage objectives. We generally refer to these as “commodity threats,” as they usually don’t have the same methodologies and persistence as APT actors.

The third domain fit the profile of a targeted attack based on the small number of victims, the types of victims sending phone-home requests, and the details in the WHOIS data. Figure 3 shows two targeted victim organizations associated with this domain, with a total of three infected systems. We identified one of the victims as a high-profile international organization using the X-Forwarded-For HTTP header’s inclusion of the organization’s URL and the internal IP address of the infected system. Two infected computers from the other unidentified organization phoned home to our sinkhole.

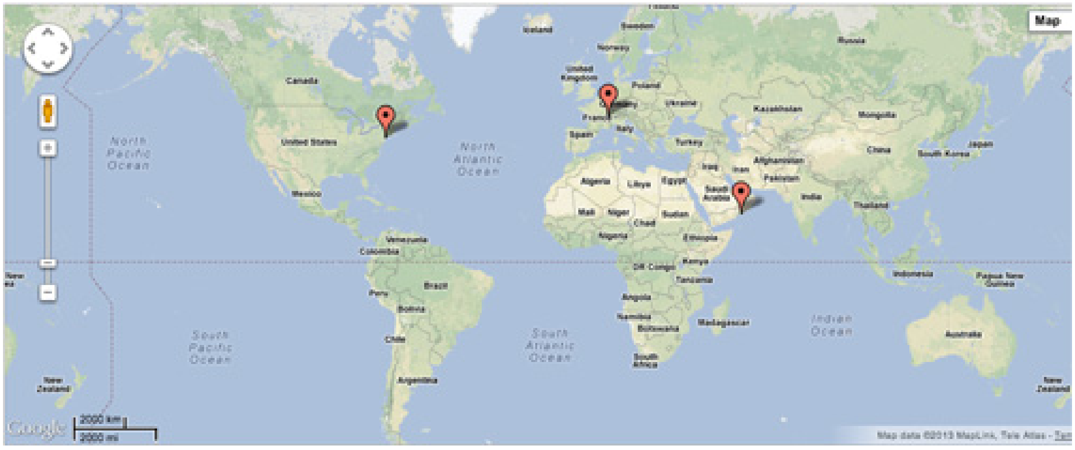


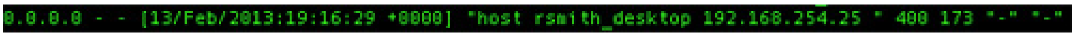
Figure 3. Infected hosts that are attributable to possible targeted attacks. (Source: Dell SecureWorks)

We reached out to the first victim in late January 2013. We provided them with all relevant data so they could remove the infection.

Often, identifying targets of these campaigns is based on either spearphishing corpuses or victim names in DNS addresses. These methods are useful for predictions and directing research, but they are speculative. This information does not include data about the success or failure of the attacks. Our sinkholing efforts provide a new perspective that can give us insight and greater certainty about the victim’s identity.

Unknown Malware Used to Target a U.S.-Based University

In late 2012, the CTU research team took control of a domain used by a group of hackers known for its APT activity. We acquired the domain after its expiration. Our analysis of the traffic directed to the domain revealed an infection originating from a large university in the United States. The unknown malware sample phoned home using Secure Sockets Layer (SSL) encryption, which complicates detection at the network level. The malware sent the hostname (rsmith_desktop) and IP address (192.168.254.25) of the infected host as shown in Figure 4.



```
0.0.0.0 - - [13/Feb/2013:19:16:29 +0000] "host rsmith_desktop 192.168.254.25 " 400 173 "-" "-"
```

Figure 4. Example phone-home request substituting non-victim data. (Source: Dell SecureWorks)

We correlated this activity to a malware family the CTU research team named Busesel. After identifying that these connections were unlikely from a malware sandbox or open proxy, we contacted the victim university’s security team and provided data we observed from our sinkholing related to their IP address. Initially, we only knew the IP address the infected system phoned home to and the structure of the phone-home request. We didn’t know the domain used for phone-home traffic, the associated MD5 hashes, or the threat actors behind the attack.

The university supplied us with Domain Name System (DNS) logs. These logs enabled us to link the activity to a malware sample that was deployed as a payload dropped by malware domains related to the Comment Group. Based on the Comment Group’s usual objectives, targeting a student or professor seemed unlikely. After reanalyzing the data in the phone-home request and researching the university activities, we believe that the intended target of the campaign was the university’s research laboratory, which does military research projects, in addition to others.

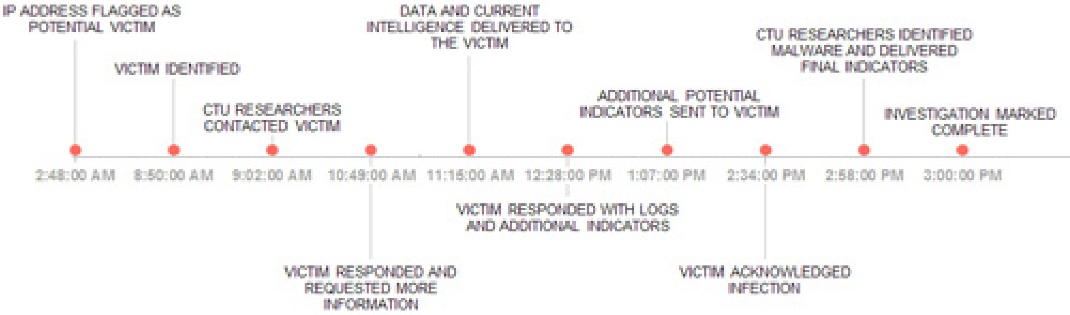

IP ADDRESS FLAGGED AS POTENTIAL VICTIM
VICTIM IDENTIFIED
CTU RESEARCHERS CONTACTED VICTIM
DATA AND CURRENT INTELLIGENCE DELIVERED TO THE VICTIM
ADDITIONAL POTENTIAL INDICATORS SENT TO VICTIM
CTU RESEARCHERS IDENTIFIED MALWARE AND DELIVERED FINAL INDICATORS
INVESTIGATION MARKED COMPLETE
2:48:00 AM
8:50:00 AM
9:02:00 AM
10:49:00 AM
11:15:00 AM
12:28:00 PM
1:07:00 PM
2:34:00 PM
2:58:00 PM
3:00:00 PM
VICTIM RESPONDED WITH LOGS AND ADDITIONAL INDICATORS
VICTIM RESPONDED AND REQUESTED MORE INFORMATION
VICTIM ACKNOWLEDGED INFECTION

Figure 5. Timeline of events surrounding CTU disclosure to the university. (Source: Dell SecureWorks)

With the help of the data provided by the university, we identified several more victims related to this malware and the Comment Group. These victims include a U.S. defense contractor, a U.S.-based energy company, and an international information technology company. CTU researchers contacted affected organizations and provided data to assist with remediation efforts.

The willingness of this university to assist with our investigation allowed us to not only help them improve their perimeter security, but also identify and notify other victims. When directly contacted about an infection, victims may be apprehensive because of the lack of pre-established trust relationships. However, overcoming the initial hesitation produces a mutual, beneficial relationship. Both sides gain the collective learned knowledge, and the victim can use the intelligence to expand their security posture.

Final Thoughts

As an Internet community, we must make a collaborative effort to share knowledge among each other to help defend against these APT threats. If we don’t, then we will surely see continued success by these highly organized and motivated APT hacker groups. Every organization has a responsibility to be a part of the broader community and not let ego drive a tradition of isolationism.

Category: **CTU Research** | By: **Silas Cutler** | On: **03/08/2013**

Like 0 +1

Post navigation

← SQL Slammer – 10 years later PCI DSS Requirement 8.3: What is two-factor authentication, and when is it required? →

Leave a Reply

You must be logged in to post a comment.

Online Tools

- Print this Page
- Share This Resource

0

Printed from

Recent Posts

- Vulnerability Assessments versus Penetration Tests
- To Bring Your Own Device, Or Not, That is the Question
- Skimmers: Telling Fact from Fiction
- 5 Valuable Contextual Data Sources for Small Businesses
- Exploiting Threat Intelligence

http://www.secureworks.com

For more information call (877) 838-7947 or email info@secureworks.com.

Have a security specialist contact you.

*First Name:

*Last Name:

*Company:

*Telephone:

*Email:

*Country: Select Country ▼

*State/Province: Select State ▼

*What is your primary role?

Please Select One ▼

*Industry: Please Select One ▼

*What is the biggest security challenge your organization is currently facing?

Please Select One ▼

Questions/Comments:

Send Request

By completing this form you'll be opting in to receiving future communications about products and services from Dell SecureWorks.

Categories

- Compliance (32)
- CTU Research (111)
- Events (7)
- Executive Insights (2)
- Information Security (130)
- & IT Security (53)