ANALYSIS BRIEF – December 2012

Modeling Exploit Evasions in Layered Security

HOW TO GRAPHICALLY REPRESENT A FUTURE DISASTER AND FOCUS ON WHAT MATTERS MOST

Authors – Francisco Artes; Stefan Frei, PhD

Overview

Maltego is a program that can be used to determine the relationships and real world links between many things, and has been adapted by NSS Labs to show the relationship and correlation of unblocked exploits through a layered security stack of hardware and software tools. Utilizing the empirical data collected during NSS Labs' tests on next generation firewalls (NGFW), intrusion prevention services (IPS), breach detection systems (BDS), endpoint security, browser security, and antivirus engines, paired with data on exploit availability of popular crimeware kits or penetration testing tools (e.g. Metasploit) NSS Labs is able to model layered defense stacks and illustrate exploits that are able to evade detection by the entire stack. NSS Labs can also simulate popular or customer specific software portfolios, allowing mapping simulations specific to their infrastructure environment.

Utilizing the relationship mapping capabilities of Maltego, it is possible to correlate results from multiple tests and infer dependencies that were not visible from the standard charts and tables. Models can be created to represent the current deployment of devices and software within a specific environment. From those models NSS can determine which current evasion techniques are capable of bypassing which security devices, and which exploits will be effective against which workstations and servers. Hardware or software can be swapped in and out of the model to simulate and illustrate changes in the security posture.

This is all possible due to the correlation of undetected exploits through the layers of the stack. Even within a single layer there is often correlation of exploitable vulnerabilities across the major vendors. For example, of the fifteen vendor-tuned IPS devices tested by NSS in 2012, eleven can be bypassed by the same exploit, identified as 2008-038 by NSS Labs. There is only one combination of two layered IPS devices that would block all currently tested exploits.

Modeling allows CISO/CSOs to identify and properly address exposures within the infrastructure for which they are responsible.

NSS Labs Findings:

- The assumption that P_A x P_B = $P_{A \circ B}$, where "P_X" is the protection failure rate by a given layer/device, is incorrect due to correlation in vulnerabilities between layered devices.

- Breach detection systems (BDS) should be added to the security infrastructure to assist with mitigating damage from side-channel attacks.
- 18% of the exploits used in NSS Labs testing are available in either Metasploit or popular crimeware kits.

NSS Labs Recommendations:

CIO/CISOs and key Information Technology/Security team members should assume their organization is already compromised. They should use NSS modeling to:

- Model replacement stack components (firewalls, NGFW, IPS, BDS, endpoint security, etc.) to visualize risks and determine future overall security effectiveness.
- Identify valid risks by modeling the current stack, allowing resources to be focused on mitigation of true risks.
- Model additional stack components to identify the key actions needed to improve overall security effectiveness.

Analysis

Given the empirical data that is collected by NSS Labs during testing, engineers are able to simulate and run test models of network security stacks. NSS Labs defines a "stack" as being the layered defenses starting from the perimeter of the network and ending within the applications and security tools of a workstation or server.

These models are graphically represented, and allow NSS Labs analysts to extrapolate and demonstrate exploits that will bypass any given stack as a result of the inability of devices or software (collectively "security systems") to recognize the exploit. Referred to as an "unrecognized exploit," these exploits easily evade the security systems. Due to the overlap in unrecognized exploits within the disparate security systems, it is important to identify those overlaps within the stack.

This data is important to the CIO/CISO and key Information Technology/Security team members since it allows them to model replacement stack components (such as firewalls, NGFW, IPS, and BDS), visualize risk, and simulate overall security effectiveness. Simulations of the current security stack provide focus on true gap mitigation for Information Technology / Security teams, and those simulations can be augmented to provide results that reflect the addition of new security components.

NSS Labs research provides that the often used formula for *protection failure rate*, $P_A \times P_B = P_{A \circ B}$, does not hold true. Rather, combined failure rates are considerably higher: $P_{A \circ B} > P_A \times P_B$. This is due to the correlation of exploits between the disparate layers of the security stack. For example, unrecognized exploits unblocked by an IPS are also missed by an NGFW, and eventually by the endpoint security software. Given the difficulties associated with patch management, it remains important to intercept exploits and mitigate security exposures on the wire rather than allow them to reach the endpoint.

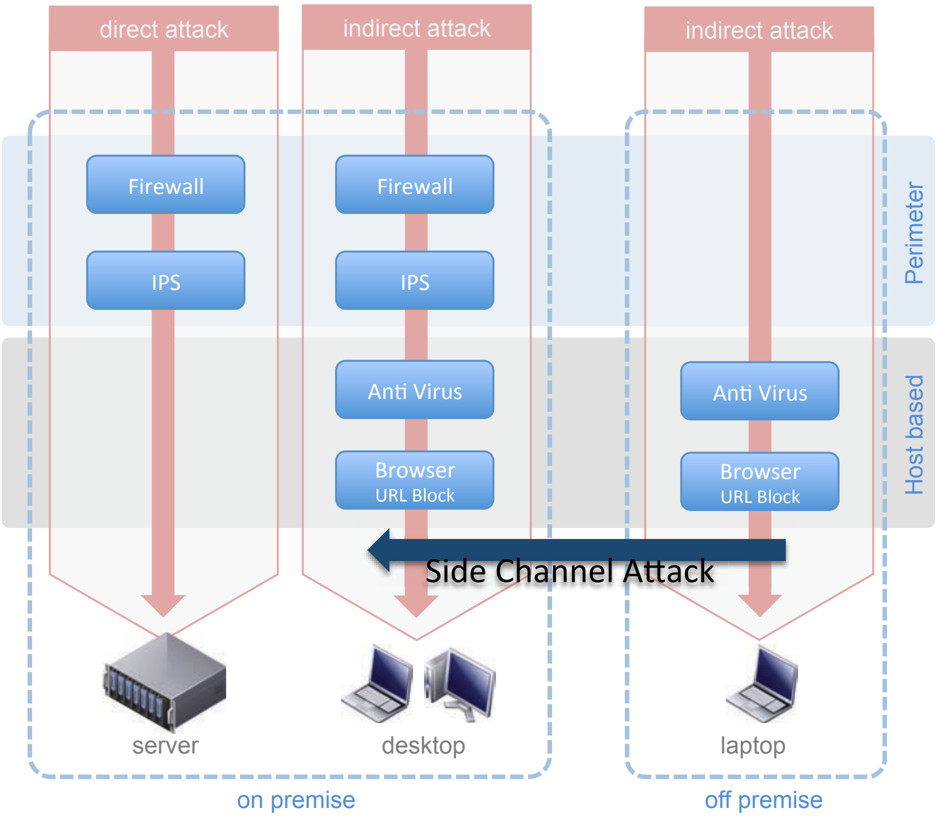


Figure 1 - Example of Layered Security and Common Attack Vectors

Side-channel attacks are defined as those that arise from infected mobile devices being reintroduced to the secure network, and are a growing reality in today's critical infrastructure security. This growth in prevalence is partially a result of BYOD implementations, as well as laptops returning to the network from business trips. These attacks are generally more potent due to the attack vector coming from behind perimeter security appliances such as IPS, NGFW, and WAF. Technologies such as BDS should be introduced to the overall security infrastructure with the goal of identifying machines infected with malware. Thus their role is one of identifying when a security perimeter has been breached, and enabling early remediation. Intelligence gained through modeling such attack vectors will enable enterprises to develop endpoint updating / patching and security processes that address critical exposure points.

Stack Modeling Example

The following examples show the output from NSS Labs unique stack modeling capability. ***Note:*** These are based on live data as of 11/2012, and CVE numbers have been replaced with "NSS IDs" in order to conceal the exact nature of those exploits that can bypass the products illustrated in the example. It is also important to keep in mind that the data being modeled is from security appliances configured and tuned by each respective vendor's top engineers. Modeling can also be presented with the default state of the appliance as delivered from the vendor to a new customer.

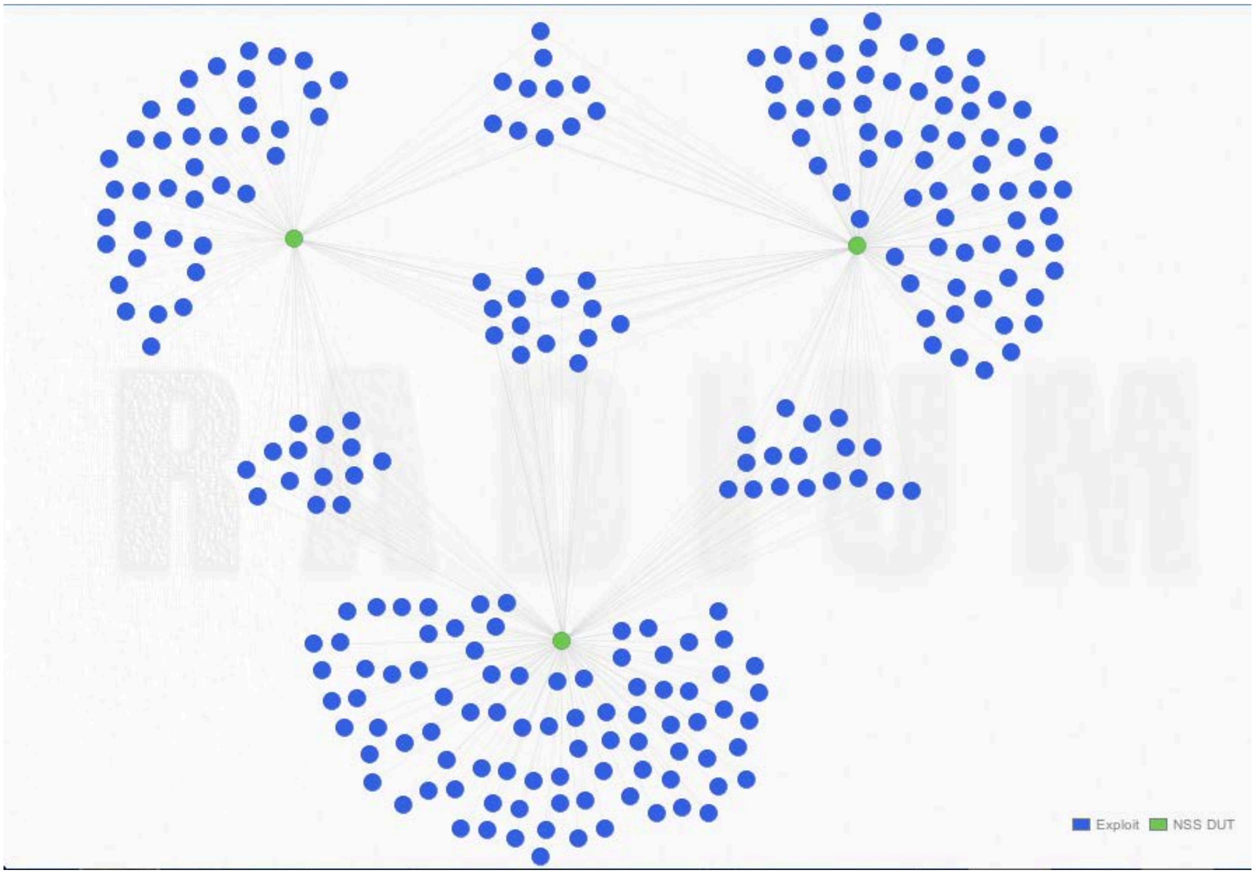


Figure 2 - High-Level Unrecognized Exploit Correlation

In Figure 2 are three devices under test (DUT) as represented by the green dots. These are a next generation firewall (NGFW), intrusion prevention system (IPS), and an endpoint security / antivirus system. The blue dots represent each exploit that was not detected by a DUT. Between any pair of DUT icons are those exploits unrecognized by each of the DUTs in that pair. Most importantly, the correlated unrecognized exploits in the middle of the graphic are those that would bypass the entire layered defense of this modeled company.

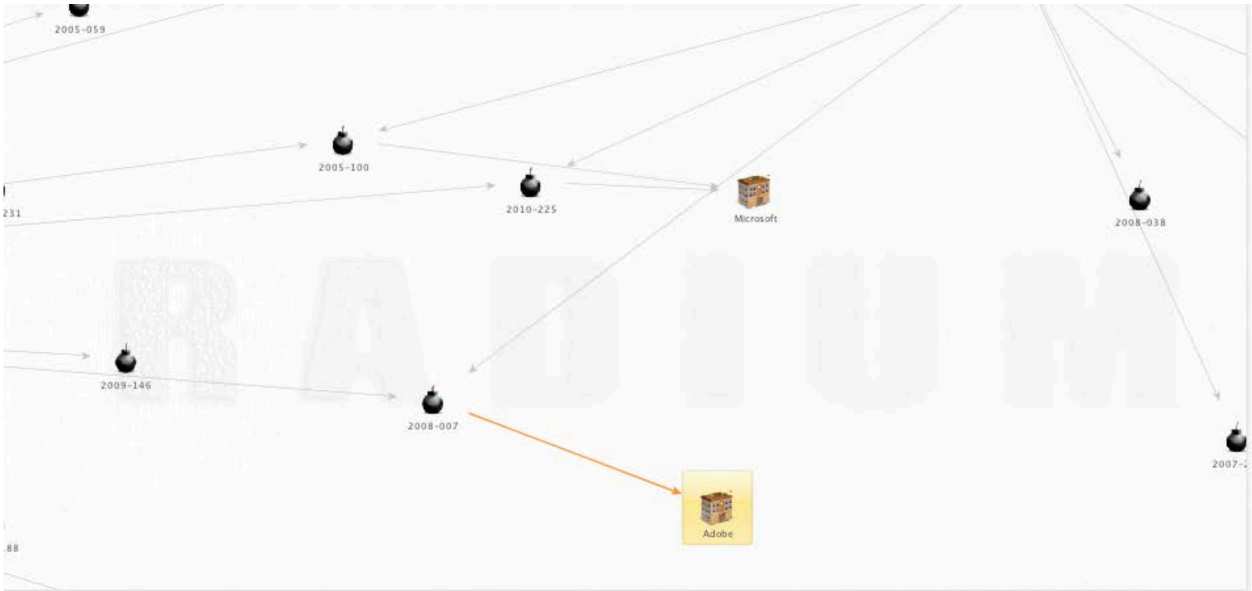
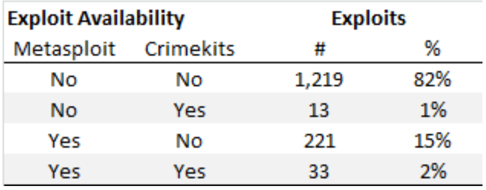


Figure 3 - Exploit to Vendor

On zooming into the data, the colored dots are replaced with icons that display the exploit ID (in this case the “NSS ID” has been used.) Once the correlated unrecognized exploits have been isolated, the next step would be to determine the platform (categorized by vendor) targeted by these exploits. As seen in Figure 3, two of the given exploits target Microsoft and one targets Adobe products. This allows for the removal of false-positive threats, e.g. those vendors that are not utilized within the actual target network. It also provides the key exploits that need to be addressed by the Information Technology / Security group.

This methodology further allows mapping and identification of exploits that are used in popular crimeware kits or penetration testing tools. Such exploits are readily available to criminals and easy to deploy through the respective tools.



Exploit Availability		**Exploits**	
Metasploit	Crimekits	#	%
No	No	1,219	82%
No	Yes	13	1%
Yes	No	221	15%
Yes	Yes	33	2%

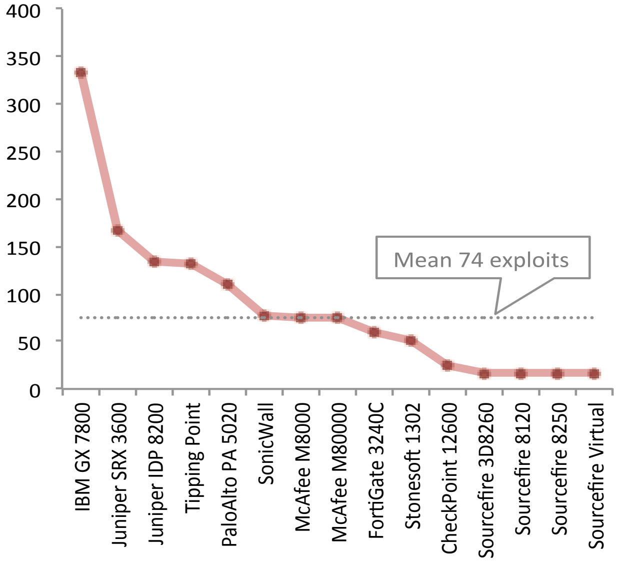
Figure 4 - Prevalence of Undetected Exploits to Common Security Tools

Figure 4 shows that at least 18% of the exploits used in NSS Labs testing are available in either Metasploit or popular crimeware kits.

Visualization of NSS Labs’ 2012 IPS Exploit Data

In Q3 of 2012, NSS Labs published the group test results for IPS. Fifteen vendor products were tested against 1,486 exploits. For measurement and evaluation purposes, NSS Labs categorizes exploits and grades a DUT based its performance in each category. The effect on the overall grade of the DUT is more severe should it fail to recognize exploits in multiple categories, as this would put the consumer at greater risk than with a DUT that fails only a few exploits from a single category. When modeling threat exposure, however, it is important to identify each exploit individually and track its performance through the layered security stack.

When reviewing the exploits individually NSS Labs' data reveals that eleven of the fifteen tested IPS products can be bypassed by the same exploit, identified as 2008-038 by NSS Labs. When modeling scenarios of stacked IPS devices, admittedly a deployment scenario beyond the reach of most consumers, there is one combination of two of the fifteen different devices that results in successfully blocking all 1,486 exploits.



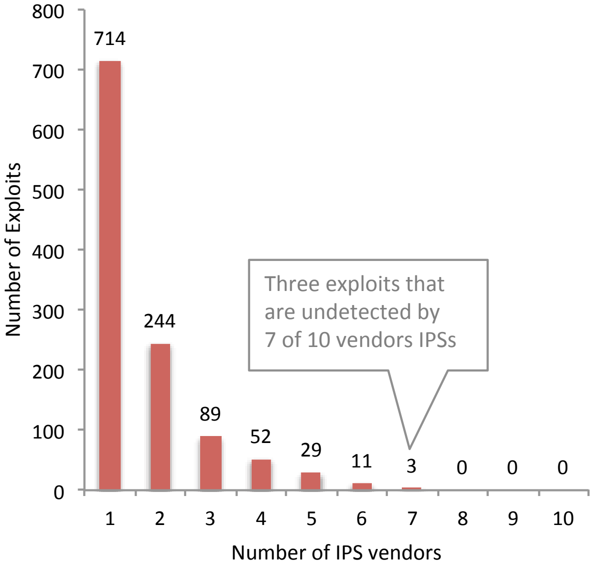


Figure 5 - Undetected Exploits by Tested Product

Figure 6 - Unique Exploits Undetected by "N" Vendor's IPS

Figure 5 represents the number of undetected exploits by products tested during the 2012 IPS Group Test. The mean is 74 exploits undetected. These numbers reflect a fully tuned device by an expert engineering resource provided by the vendor. Preliminary testing prior to the tuning (i.e. with a default policy) reveals 50% lower protection then the results presented in Figure 4. These block rates vary between 77% and 98% effectiveness.

Figure 6 illustrates the dispersion of undetected exploits over the number of vendors tested. During this test, three exploits were discovered that are unindentified by seven of the ten tested vendors. These seven vendors represent over 90% of the market share of deployed IPS.

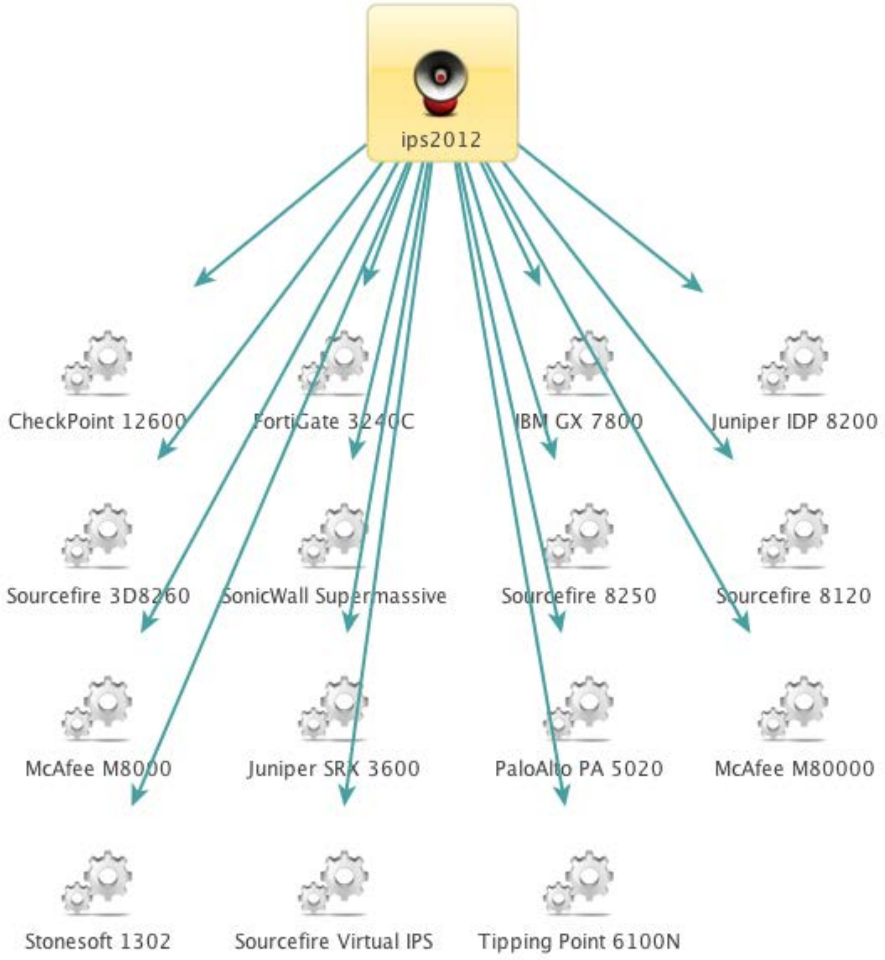


Figure 7 - DUT Pulled from Test Results

Figure 7 shows the results from the NSS Labs 2012 IPS test results and the devices within the database that are associated to that test as reported by the NSS Labs custom Maltego transform. Transforms are programs added to the base Maltego software that allow the entities (displayed information) to be modified and manipulated. The NSS Labs transforms map the tests to DUTs, exploit data to DUTs, exploits to vendors and vice-versa. While this example is of a single test, other complete tests (or individual devices) could be included for more extensive modeling.

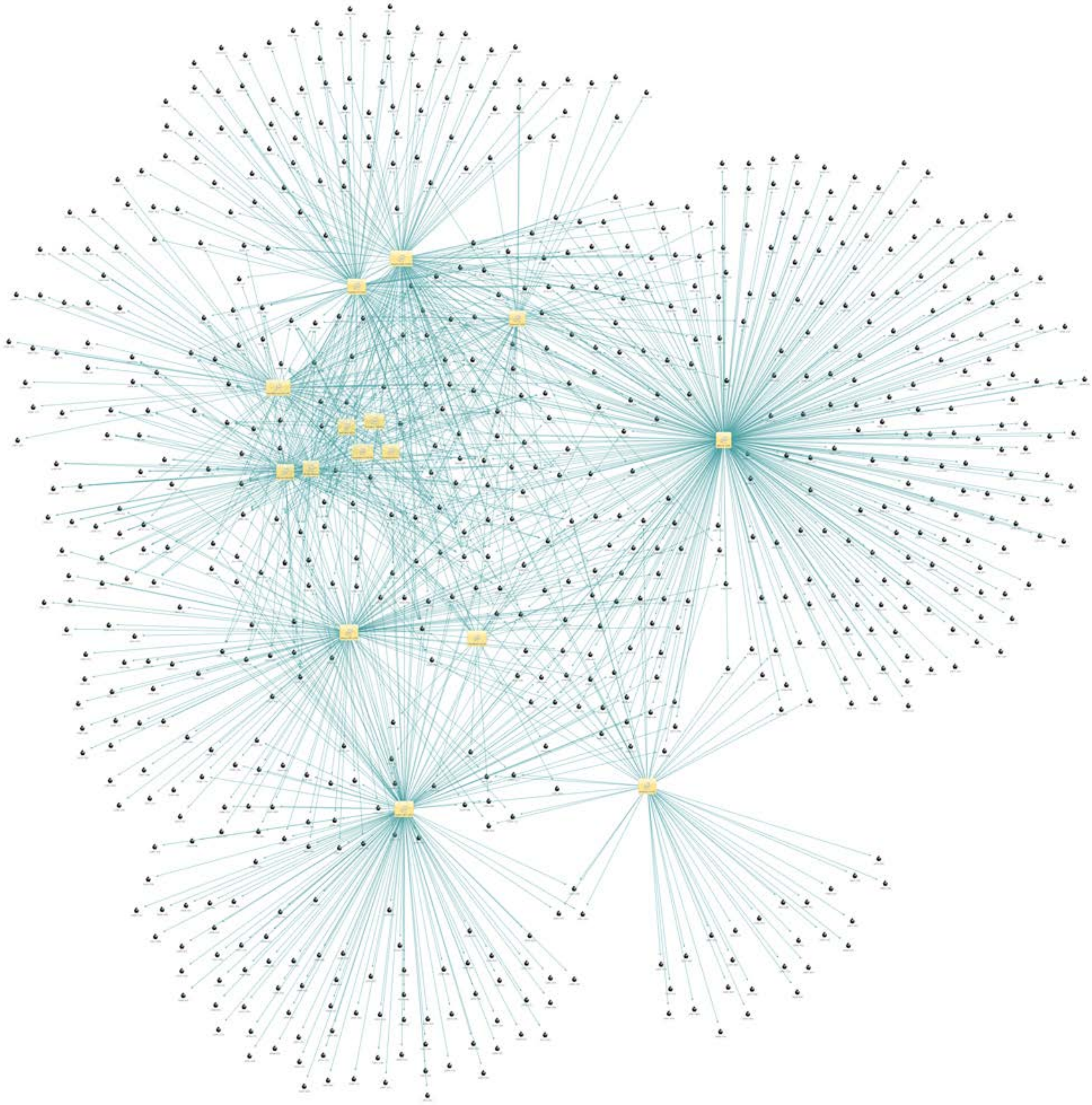


Figure 8 - Exploits Explode

While modeling only the IPS 2012 devices, the next step in modeling involves running transforms that mine the databases to present the undetected exploits by product. Maltego utilizes the Node ID of each object to show how it is connected and interconnected (both incoming and outgoing connections) to other objects in the data map. The DUT are represented by the yellow rectangles, and the exploits by black dots. This view is zoomed out to show the number and overall cross-connection of the exploits. Weighting can be applied allowing the dots to grow in size, each getting larger based on the number of connections it has. Exploits with multiple connections to tested devices would be larger than those with fewer connected devices.

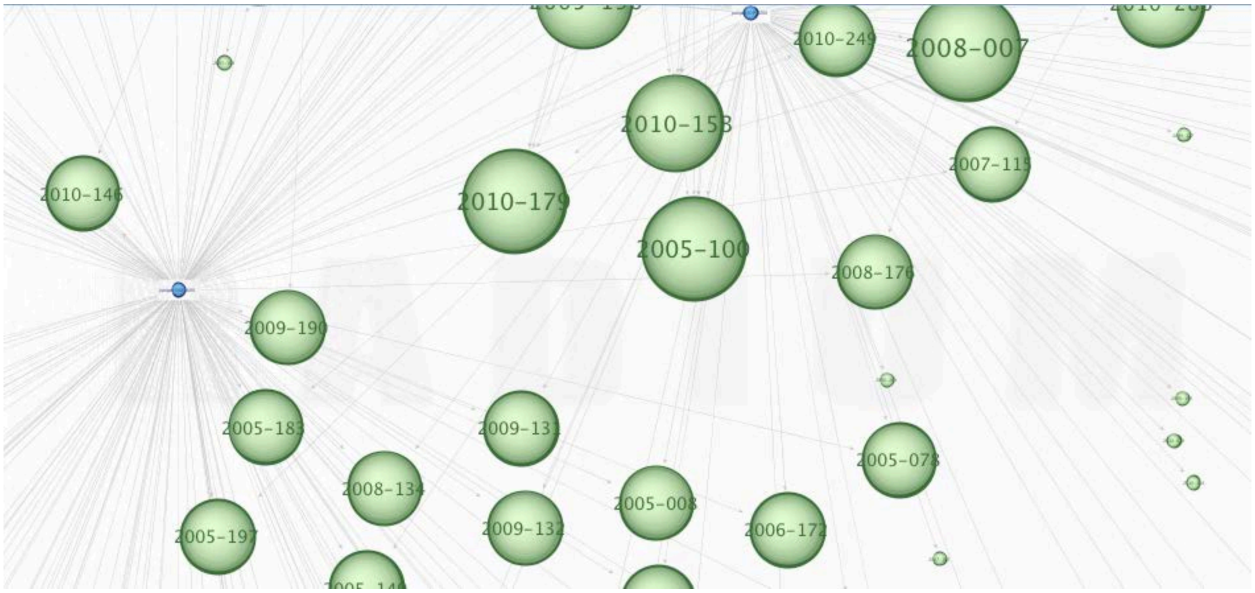


Figure 9 - A Closer Look at Exploits

Maltego permits zooming in to the wireframe; at this level the exploits are now green and are clearly weighted. The DUTs are single points and are the same size as exploits that have only one connected device. Also present are the NSS ID numbers for each exploit. This information remains confidential during modeling, but detailed exploit information can be provided to NSS clients when modeling custom environments so they may take action to mitigate risk exposure in their own organization.

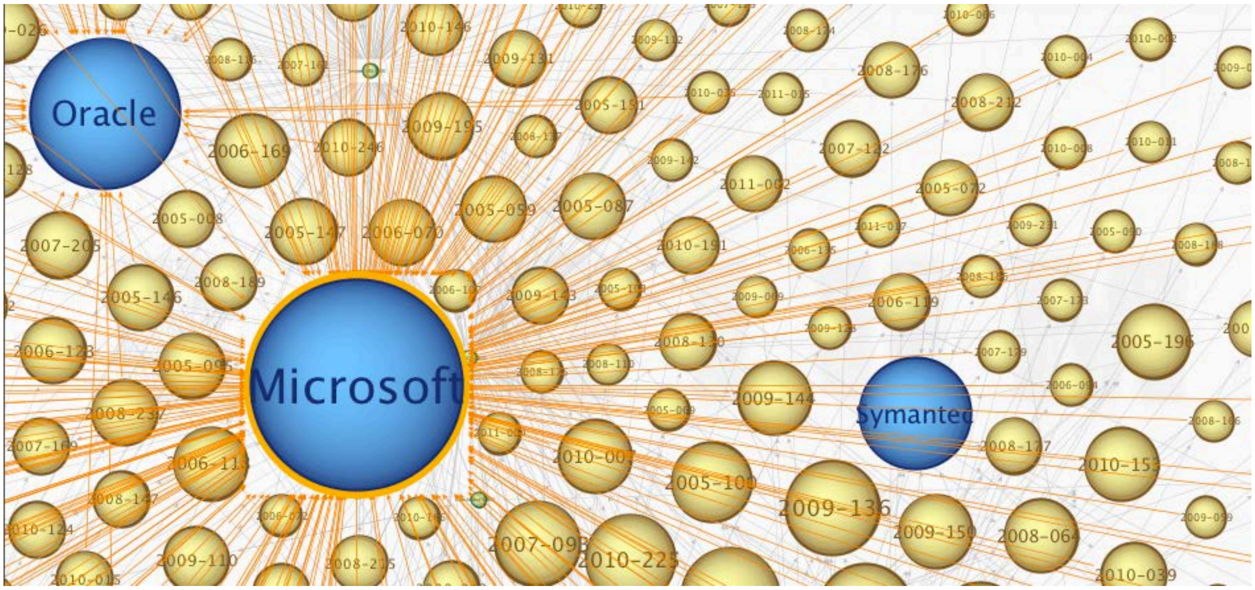
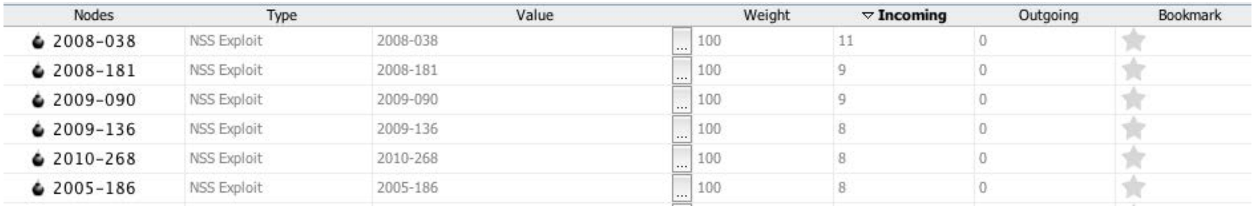


Figure 10 - Exploits with Context

Figure 10 shows results form another proprietary transform that references the vendors affected by the selected exploits. As with the earlier example, all exploits were selected and the database was polled resulting in a weighted display of vendor names. Maltego again links the objects within the wireframe and weights the objects by the number of inbound connections. It is evident that a significant number of the unrecognized exploits target Microsoft, Symantec, and Oracle applications. Note: This is a snapshot from one portion of the wireframe and is not the full list of targeted vendor products.



Nodes	Type	Value	Weight	▽ Incoming	Outgoing	Bookmark
2008-038	NSS Exploit	2008-038	100	11	0	★
2008-181	NSS Exploit	2008-181	100	9	0	★
2009-090	NSS Exploit	2009-090	100	9	0	★
2009-136	NSS Exploit	2009-136	100	8	0	★
2010-268	NSS Exploit	2010-268	100	8	0	★
2005-186	NSS Exploit	2005-186	100	8	0	★

Figure 11 - Sorting Data

Within the *Entity List* in Maltego the data is parsed by incoming connections and limited to exploits. Figure 11 demonstrates that the exploit with NSS ID 2008-038 has eleven connected devices out of the test of fifteen devices. A right-click creates a new wireframe showing the eleven devices in question (Figure 11.) This model could have begun with a single exploit and subsequently tracked which devices and software were unable to recognize the exploit; such an exercise is more offensive than it is defensive in nature, however.

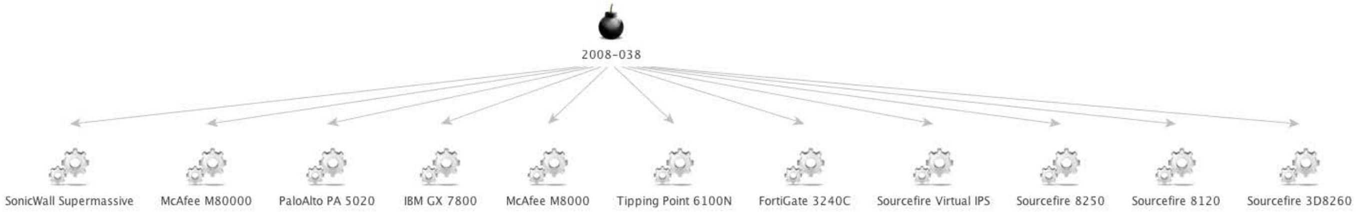


Figure 12 - Undetected Exploit Mapped to Devices

In Figure 11, NSS ID 2008-038 was found to have eleven connected IPS devices that share in their inability to identify this exploit. In Figure 12 the exploit is used as the seed for the data search, which then provides a list of vulnerable devices. An additional transform could easily take those eleven devices and display all additional exploits they may have in common. It is also possible to identify any NGFW, endpoint security, browser, and application that also fail to identify the exploit. This would result in all possible combinations of devices and software that could be bypassed by this one exploit.

This combination of unique transforms allows NSS clients to identify operating systems, services and applications that should be prioritized for patching, or which should be targeted for removal from the standard corporate software stack.

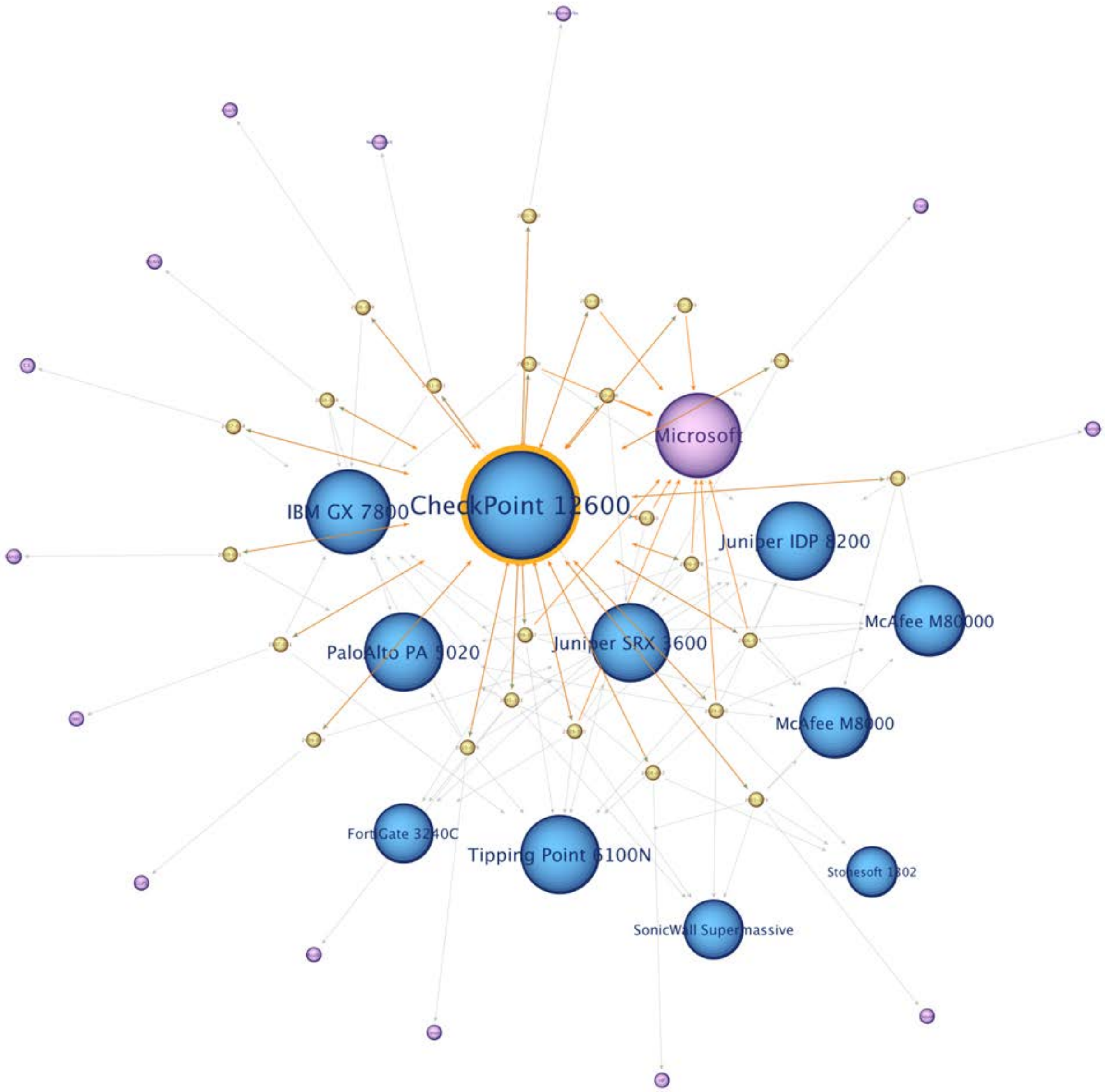


Figure 13 - Common Undetected Exploits

Figure 13 depicts a group of devices (blue) linked to one another by their common undetected exploits (yellow.) The vendors (purple) targeted by each exploit are also represented. Out of the vulnerable applications in this data model, Microsoft products are the most vulnerable to undetected exploits when protected by any of these eleven products.

Using Modeled Data

In reviewing Figure 13, a CIO/CISO would have a short list of vendor applications to target for remediation. This may require additional endpoint security, or potentially the selection of alternative or complimentary network security. In many cases it could result in a clear corporate decision to remove, for instance, something as simple as the Java JRE from all workstations. Similarly this may draw attention to the need to address patch management differently, and consequently change the urgency value given to specific applications when notified of patches or of new threats via a commercial threat feed.

Using these techniques, resources can be directed where they are truly needed. Through modeling, superfluous security devices may even be eliminated, saving a corporation valuable financial resources. While Microsoft products are the most vulnerable they may not be the largest risk to the company. There are exploits here that target McAfee, HP print servers, and Apache as well. All data must be analyzed and presented in context with the customer's security processes as well as overall infrastructure.

Reading List

Maltego, by Paterva, documentation http://www.paterva.com/web6/documentation/index.php

NSS Brief: 2012 Cybercrime Kill Chain https://www.nsslabs.com/reports/cybercrime-kill-chain-vs-defense-effectiveness

Contact Information

NSS Labs, Inc.
6207 Bee Caves Road, Suite 350
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

This analysis brief was produced as part of NSS Labs' independent testing information services. Leading products were tested at no cost to the vendor, and NSS Labs received no vendor funding to produce this analysis brief.

Please note that access to or use of this report is conditioned on the following:

1. The information in this report is subject to change by NSS Labs without notice.

2. The information in this report is believed by NSS Labs to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at the reader's sole risk. NSS Labs is not liable or responsible for any damages, losses, or expenses arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet the reader's expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.