Live Virus Testing with Virus Throttle Technology
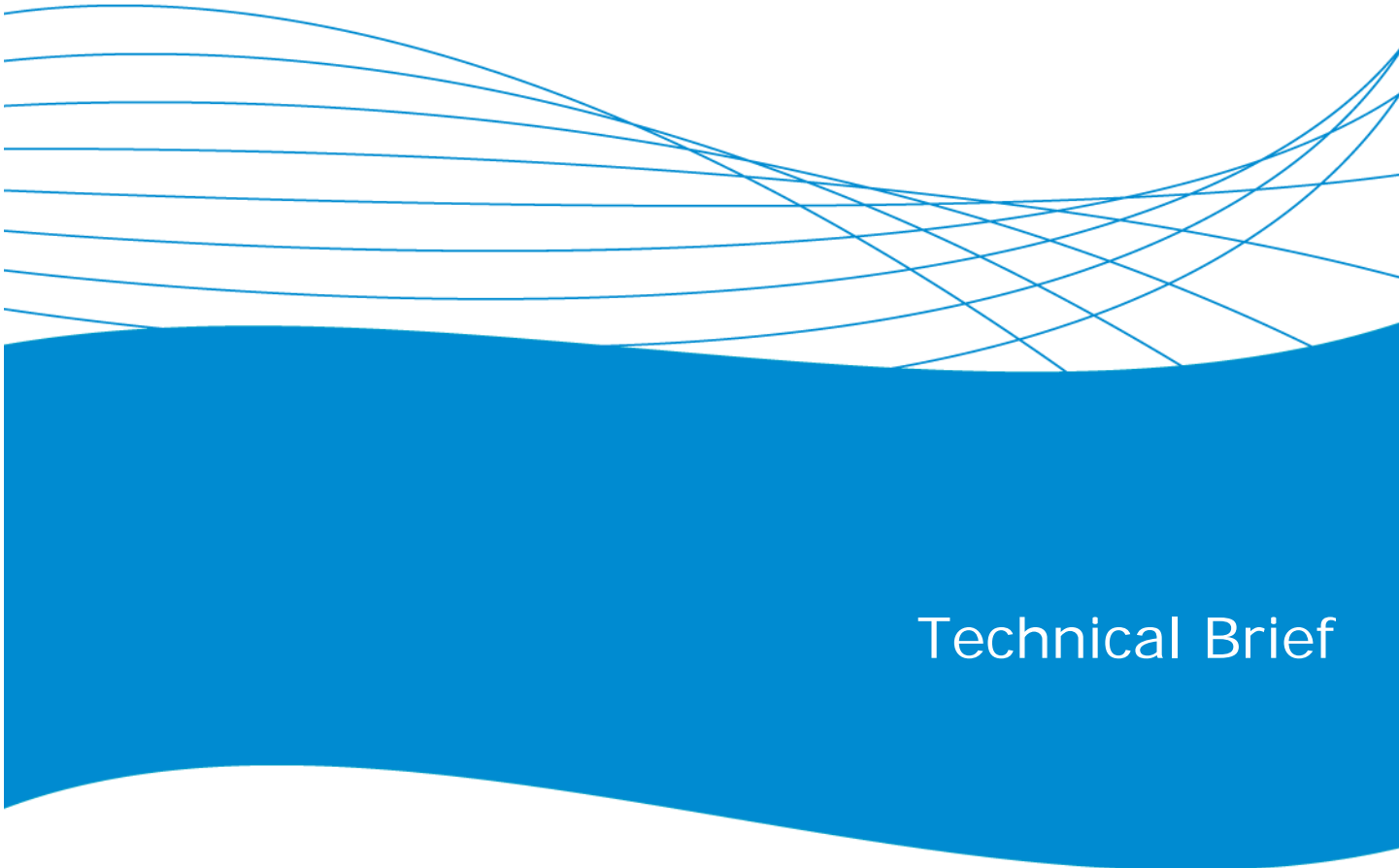
Technical Brief

Introduction

Virus Throttle (VT) technology has a powerful ability to detect and respond to real-world virus and worm attacks. Developed in HP labs, VT technology is implemented through the connection-rate filtering feature in the ProCurve Switch 3500yl, 5300xl, 5400zl, 6200yl, and 8212zl series.

Unlike traditional anti-virus approaches based on the actual code or signature of a virus, VT technology requires no signature files; therefore, it can protect networks from zero-day threats long before typical anti-virus and IPS (Intrusion Prevention System) vendors can provide any remedies.

VT technology works by intercepting all IP connection requests and putting a rate limit on connections to new computers. A computer infected with a virus – such as the well-known "Sasser" – will attempt to infect more computers on the network, thus triggering the VT technology to respond.

The flexibility of VT technology allows it to detect and respond to different types of virus attacks. Some of these actions are:

- Block – Disable the host until an administrator explicitly re-enables access.
- Notify-only – Log a message/send a SNMP trap when the filter is tripped.
- Throttle – Deny network access for a period before automatically re-enabling access.

In technical terms, a virus is defined as having to be executed by something, while a worm is self-propagating. To eliminate confusion, the terms "virus" and "worm" will be used synonymously throughout this tech brief. Each of the viruses listed below are considered to be among the top threats in recent years. They were chosen because they are frequently listed on anti-virus vendor's top threat lists, and have captured significant media attention due to the substantial monetary damages incurred.

Listed below are seven "top threat" viruses, along with brief descriptions of each – including their reported frequency and resulting monetary impact. The monetary values are calculated by security researchers on the basis of help desk support costs, overtime payments, contingency outsourcing, loss of business, bandwidth clogging, productivity erosion, management time reallocation, cost of recovery, and software upgrades. While these values are approximations, it is important to note these viruses continue to infect computers today and cause continued loss.

- **Bagle** - A mass-mailing worm that spreads through file-sharing networks. The worm also will open a backdoor to allow unauthorized access. This was the #6 virus reported by Sophos on its top 10 list for 2006; it accounted for 5.5 percent of reports for that year. Estimated economic damage: "between $733 million and $896 million dollars."[1]

- **Blaster** – A network worm that propagates by exploiting the critical security vulnerability found in the DCOM RPC interface buffer overrun within Microsoft Windows 2000 and XP. Some variants are known to launch Denial of Service (DoS) attacks against web sites and open up a back door allowing unauthorized access. Security firm mi2g[1] estimates that this virus has caused $32.8 billion in economic damages.

- **MyDoom** – A mass-mailing worm that propagates through e-mail. The worm acts as a Trojan, which allows unauthorized access to an infected system. Some variants are known to launch DoS attacks against web sites. According to mi2g, "MyDoom caused $37 Billion in damages."

- **Mytob** – A mass-mailing worm targeting systems running certain versions of Microsoft Windows. The worm propagates by exploiting DCOM RPC buffer overflow and Local Security Authority Subsystem Service (LSASS) buffer overflow vulnerabilities, sending a copy of itself via e-mail and network shares. This was the #1 virus reported by Sophos on its top 10 list for 2006. It accounted for 29.9 percent of reports for that year.

- **NetSky** – A mass-mailing worm that targets systems running certain versions of Windows. The worm propagates by sending itself as attachments to e-mail. Some variants copy themselves to network shares, as well as open a backdoor and perform DoS attacks. This was the #2 virus reported by Sophos on its top 10 list for 2006; it accounted for 20.8 percent of reports for that year. Security company mi2g estimated the economic damage to be at least US$3.12 billion.

---

[1] Mi2g - http://www.mi2g.co.uk/

- **Sasser** - A network worm that propagates by exploiting the critical security vulnerability found in the LSASS within Microsoft Windows. The worm propagates by scanning the network for vulnerable systems. Estimated damage: tens of millions of dollars[2].

- **Sober** – A mass-mailing worm that targets certain versions of Microsoft Windows. The worm propagates by sending itself as attachments to e-mail. This was the #3 virus reported on the Sophos top 10 list for 2006, and accounted for 17.7 percent of reports for the year.

Test Setup

A network environment resembling a customer network was designed to analyze VT technology's ability to detect malicious traffic. All viruses were injected independently into a client, and the time between the point of injection and the point of detection was measured. Virus Throttling is an integrated component of select ProCurve switches and requires no further software and hardware installations. In the test setup, the ProCurve 5406zl and ProCurve 3500yl-48g switches were used; both support Virus Throttling.

2 http://www.techweb.com/article/showArticle.jhtml?articleId=160200005&pgno=3
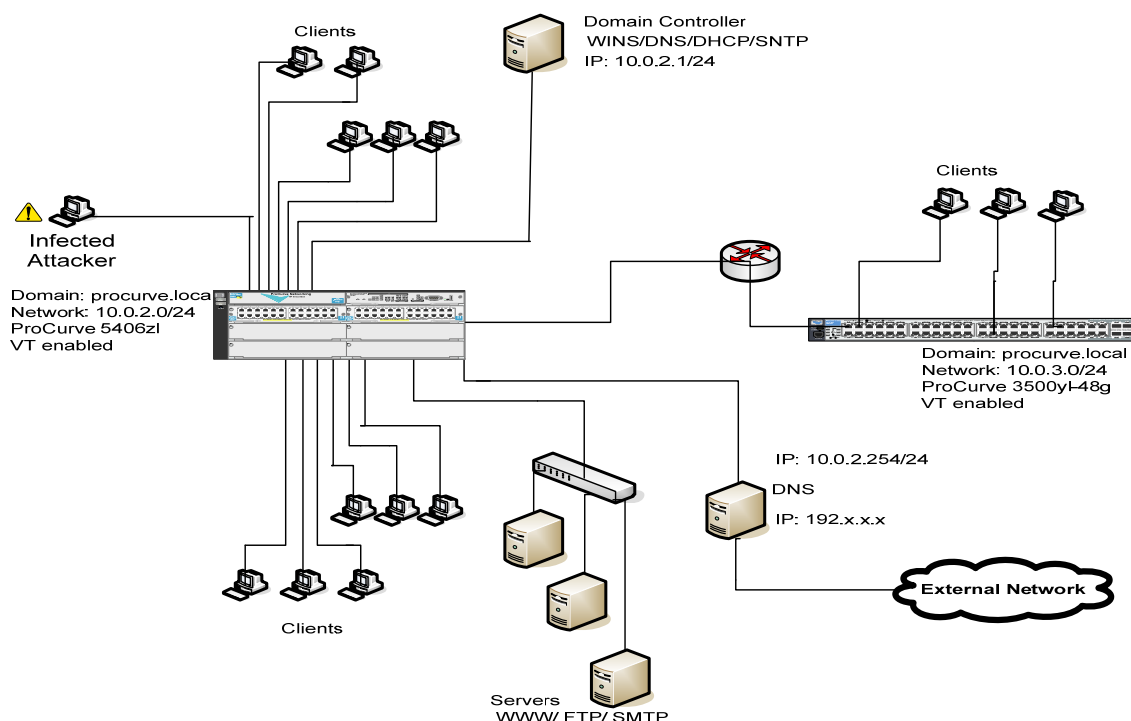
Results

Virus	Sensitivity	Detection Time (seconds)			Average Detection Time (seconds)
		Trial 1	Trial 2	Trial 3	
Bagle	Aggressive	-	-	-	-
	High	-	-	-	-
	Medium	-	-	-	-
	Low	-	-	-	-
Blaster	Aggressive	< 1	< 1	< 1	< 1
	High	< 1	< 1	< 1	< 1
	Medium	< 1	< 1	< 1	< 1
	Low	< 1	< 1	< 1	< 1
MyDoom	Aggressive	18	16	20	18
	High	-	-	-	-
	Medium	-	-	-	-
	Low	-	-	-	-
Mytob	Aggressive	< 1	< 1	< 1	< 1
	High	< 1	< 1	< 1	< 1
	Medium	< 1	< 1	< 1	< 1
	Low	< 1	< 1	< 1	< 1
Netsky	Aggressive	< 1	< 1	< 1	< 1
	High	-	-	-	-
	Medium	-	-	-	-
	Low	-	-	-	-
Sasser	Aggressive	< 1	< 1	< 1	< 1
	High	< 1	< 1	< 1	< 1
	Medium	< 1	< 1	< 1	< 1
	Low	< 1	< 1	< 1	< 1
Sober	Aggressive	-	-	-	-
	High	-	-	-	-
	Medium	-	-	-	-
	Low	-	-	-	-

Note: - Denotes data not available, VT technology was not triggered.

Sensitivity

– Low: Sets the level of connection-rate filtering to low (most permissive)

– Medium: Sets the level of connection-rate filtering to medium (permissive)

– High: Sets the level of connection-rate filtering to high (restrictive)

– Aggressive: Sets the level of connection-rate filtering to aggressive (most restrictive)

Key Statistics

Detection Time Range:

< 1 second to 20 seconds

Detecting Viruses in a Matter of Seconds

The tests allowed VT to reveal its true potential in a real world environment. VT technology was able to detect and mitigate threats quickly without the need to install and configure complex software packages. Enabling VT within ProCurve switches requires only two simple commands and can be configured in seconds.

The test environment utilizes 5400zl and 3506yl switches which supports VT technology in both bridging and routing mode. Bridging mode provides protection within a VLAN while routing mode provides protection across different VLANs. By supporting both operating modes, this enables VT technology to function within and across a VLAN, allowing VT to protect every single port on the network. While the ProCurve 8212zl and 6200yl were not used in this test, they also support both routing and bridging mode.

The 5300xl switches support VT technology in routing mode only. As a result, virus attempting to spread within a VLAN will not trigger V technology. The chance of this occurring is very small. Our results reveal that virus tends to attack random IP addresses that could span a very large range. More than likely, these IP address will span across VLANs and as a result, VT technology will trigger and provide immediate remediation to the threats. The detection rate will be the same as reported in this whitepaper. Utilizing any of the previously mentioned switches with VT enabled will provide an effective component in mitigating virus related threats.

The integration of VT technology with ProCurve switches provide customer with another means of protection from the core to the edge. ProCurve recommends that customers use VT technology along with a network based anomaly and signature technologies such as those found in the ProCurve Network Immunity Manager to provide a complete threat management solution for their networks.

VT technology detected five out of seven viruses in a matter of seconds. History has proven that viruses like Sasser, Blaster and Mytob which spread extremely fast in networks can be difficult to isolate. Traditional anti-virus software was not be able to mitigate these threats at initial exposure, causing huge catastrophes resulting in business downtime and huge monetary loses. However, with VT technology, threats such as these were being detected and mitigated in milliseconds upon first exposure inside the network.

While the result is promising, it is important to understand why the Bagle and Sober viruses went undetected. After careful analysis of each virus' activities, it was determined that the slow propagation rate of Bagle and Sober is what allowed them to go undetected. To mitigate these threats, ProCurve Network Immunity Manager software has been successfully tested to detect these viruses using network behavior anomaly detection on sampled traffic using sFlow technology.

The method of propagation for Bagle is through e-mail. The virus attempted to establish connections at a rate between one to six connections per second with an average of three packets per second. This connection-rate range is typical in a normal network environment; therefore, the virus will not trigger VT technology.

A portion of the packet capture screenshot shown below illustrates the activity of the Bagle virus. The infected host with a source address of 10.0.2.17 attempts to make SMTP (e-mail) connections to multiple destinations. Despite the number of connections the virus tries to establish, it does so at a slow rate.

No.	Time ▾	Source	Destination	Protocol	Info
475	71.172547	10.0.2.17	128.121.50.122	TCP	1134 > smtp [SYN] Seq=0 Len=0 MSS=1460
476	71.390544	10.0.2.17	128.121.79.138	TCP	1135 > smtp [SYN] Seq=0 Len=0 MSS=1460
477	71.610668	10.0.2.17	209.87.252.178	TCP	1136 > smtp [SYN] Seq=0 Len=0 MSS=1460
478	75.540404	10.0.2.17	198.175.230.35	TCP	1137 > smtp [SYN] Seq=0 Len=0 MSS=1460
479	75.759307	10.0.2.17	198.175.230.33	TCP	1138 > smtp [SYN] Seq=0 Len=0 MSS=1460
480	75.977629	10.0.2.17	12.179.247.41	TCP	1139 > smtp [SYN] Seq=0 Len=0 MSS=1460
481	77.946900	10.0.2.17	84.17.190.210	TCP	1141 > smtp [SYN] Seq=0 Len=0 MSS=1460
482	78.164713	10.0.2.17	64.26.62.254	TCP	1142 > smtp [SYN] Seq=0 Len=0 MSS=1460
483	81.226406	10.0.2.17	84.17.190.210	TCP	1141 > smtp [SYN] Seq=0 Len=0 MSS=1460
484	81.445010	10.0.2.17	64.26.62.254	TCP	1142 > smtp [SYN] Seq=0 Len=0 MSS=1460
485	82.623234	10.0.2.17	83.243.58.182	TCP	1143 > smtp [SYN] Seq=0 Len=0 MSS=1460
486	84.083863	10.0.2.17	128.121.50.122	TCP	1144 > smtp [SYN] Seq=0 Len=0 MSS=1460
487	84.309518	10.0.2.17	128.121.50.122	TCP	1145 > smtp [SYN] Seq=0 Len=0 MSS=1460
488	84.515610	10.0.2.17	128.121.79.138	TCP	1146 > smtp [SYN] Seq=0 Len=0 MSS=1460
489	84.723263	10.0.2.17	209.87.252.178	TCP	1147 > smtp [SYN] Seq=0 Len=0 MSS=1460
490	85.924305	10.0.2.17	83.243.58.182	TCP	1143 > smtp [SYN] Seq=0 Len=0 MSS=1460
491	87.337644	10.0.2.17	128.121.50.122	TCP	1144 > smtp [SYN] Seq=0 Len=0 MSS=1460
492	87.556822	10.0.2.17	128.121.50.122	TCP	1145 > smtp [SYN] Seq=0 Len=0 MSS=1460
493	87.775273	10.0.2.17	84.17.190.210	TCP	1141 > smtp [SYN] Seq=0 Len=0 MSS=1460
494	87.775283	10.0.2.17	128.121.79.138	TCP	1146 > smtp [SYN] Seq=0 Len=0 MSS=1460
495	87.994561	10.0.2.17	64.26.62.254	TCP	1142 > smtp [SYN] Seq=0 Len=0 MSS=1460
496	87.994573	10.0.2.17	209.87.252.178	TCP	1147 > smtp [SYN] Seq=0 Len=0 MSS=1460
497	88.641269	10.0.2.17	198.175.230.35	TCP	1148 > smtp [SYN] Seq=0 Len=0 MSS=1460
498	88.851148	10.0.2.17	198.175.230.33	TCP	1149 > smtp [SYN] Seq=0 Len=0 MSS=1460
499	89.118669	10.0.2.17	12.179.247.41	TCP	1150 > smtp [SYN] Seq=0 Len=0 MSS=1460
500	91.887478	10.0.2.17	198.175.230.35	TCP	1148 > smtp [SYN] Seq=0 Len=0 MSS=1460
501	92.106320	10.0.2.17	198.175.230.33	TCP	1149 > smtp [SYN] Seq=0 Len=0 MSS=1460
502	92.323813	10.0.2.17	12.179.247.41	TCP	1150 > smtp [SYN] Seq=0 Len=0 MSS=1460
503	92.433774	10.0.2.17	83.243.58.182	TCP	1143 > smtp [SYN] Seq=0 Len=0 MSS=1460
504	93.839737	10.0.2.17	128.121.50.122	TCP	1144 > smtp [SYN] Seq=0 Len=0 MSS=1460
505	94.056848	10.0.2.17	128.121.50.122	TCP	1145 > smtp [SYN] Seq=0 Len=0 MSS=1460
506	94.265843	10.0.2.17	128.121.79.138	TCP	1146 > smtp [SYN] Seq=0 Len=0 MSS=1460
507	94.484812	10.0.2.17	209.87.252.178	TCP	1147 > smtp [SYN] Seq=0 Len=0 MSS=1460
508	98.433328	10.0.2.17	198.175.230.35	TCP	1148 > smtp [SYN] Seq=0 Len=0 MSS=1460
509	98.661671	10.0.2.17	198.175.230.33	TCP	1149 > smtp [SYN] Seq=0 Len=0 MSS=1460
510	98.923914	10.0.2.17	12.179.247.41	TCP	1150 > smtp [SYN] Seq=0 Len=0 MSS=1460
511	100.893687	10.0.2.17	84.17.190.210	TCP	1151 > smtp [SYN] Seq=0 Len=0 MSS=1460
512	101.112445	10.0.2.17	64.26.62.254	TCP	1152 > smtp [SYN] Seq=0 Len=0 MSS=1460

Another virus not detected by VT technology was Sober. Like Bagle, hosts infected with Sober do not generate enough connections within the specified time frame to trigger VT technology. In our test, the host infected with Sober attempted to make connections at a rate from one to three connections per second, with an average of one packet per second. The connection rate of Sober was slower than Bagle; therefore, it failed to trigger VT technology.

Sensitivity Analysis

During our virus testing, VT technology in aggressive mode was able to detect the most number of viruses. While this may seem to be the best setting to configure, network administrators should be cautious, as aggressive and high mode may generate more false positives.

Recommendations

ProCurve recommends that for large and more complex networks, VT technology should be set to low or medium. This will provide a remedy within seconds for fast-spreading viruses such as Blaster, Mytob and Sasser. Traditional methods of virus detection, which rely on definition/signature files, will fail to detect these viruses at first presence. Instead, VT technology can take action as soon as the unknown virus tries to propagate; this will significantly lower the potential financial damages.

For smaller networks where traffic is minimal, administrators can enable VT technology in aggressive and high-sensitivity mode, baring in mind the risks of false positives.

It should be noted that Virus Throttling should not be enabled on interfaces used by routers, servers and clients with P2P clients or management consoles installed. These hosts have a tendency to scan networks and make connections frequently, which could trigger VT technology.

The results clearly show the effectiveness of VT technology in preventing fast-spreading viruses from spreading across the network. This allows system administrators to have time to isolate and clean the infected hosts, preventing a widespread dilemma.

Conclusion

Traditional methods of addressing viruses and worms depend on signatures and patches. These methods are no longer effective as new viruses tend to spread across the network, often generating huge amounts of traffic and disrupting normal operations within minutes.

The VT technology focuses on the network behavior of viruses, so it can detect and respond to such threats. As a result, Virus Throttling is very effective at preventing the most destructive viruses from spreading across the entire network in a matter of seconds.

Virus Throttle technology is a unique feature built into ProCurve 3500yl, 5300xl, 5400zl 6200yl and 8212zl series switches. It allows administrators to protect their network infrastructure by slowing or stopping a virus infected host exhibiting high connection rates. Deploying virus-throttling would make it difficult for viruses to spread.

The Virus Throttling technology is a key component to the network immunity solution within ProCurve's comprehensive security vision and strategy – ProActive Defensive – to defend the network from virus and worm attacks. This assures uninterrupted network services, reducing the risks of sizably large monetary damages.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com