

WHITE PAPER
October 2009

The Anatomy of an Attack

The re-emergence of attacks we thought had disappeared.

ABSTRACT

Hackers are returning to once forgotten exploits to gain access to corporate networks. This white paper explores the anatomy of these attacks and proposes an explanation for why they are once again on the increase.

Author

Toby Scott-Jackson
Head of Compliance

Introduction

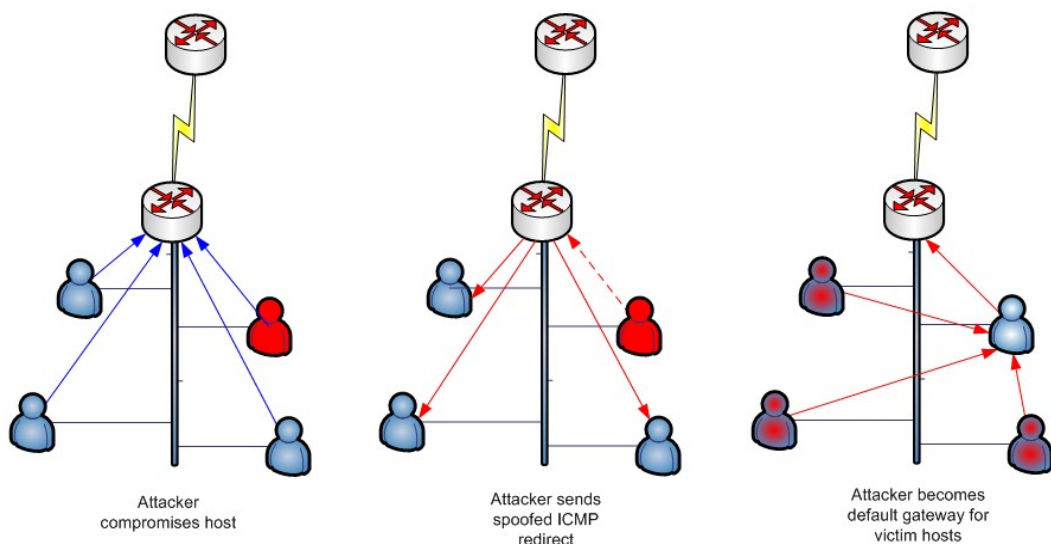
Over the past twelve months SureCloud has been monitoring a strange occurrence; the re-emergence of old attacks, the security community thought they had seen the back of. This white paper will look at some of the attacks that have been re-emerging and will explain why SureCloud believes hackers are reverting to these types of attacks to infiltrate network perimeters.

Attack Types

ICMP Redirect Spoofing

ICMP is the protocol that enables the internet to function correctly. ICMP attacks are often overlooked these days, but can be very powerful if deployed correctly, especially if the attacker has managed to compromise a device capable of packet forwarding. ICMP attacks using spoofed redirects and router solicitation enable the attacker to perform 'man-in-the-middle' attacks, redirecting network traffic through the attacker's compromised device. Other, common ICMP attacks including the Smurf attack can cause widespread network Denial of Service (DoS) for both the target organisation and other organisations used as Smurf Amplifiers.

See: <http://www.cert.org/advisories/CA-1998-01.html>



UDP Spoof Attacks

Because of its connectionless state, UDP is particularly susceptible to spoofed packet attacks, especially because of the lack of RFC1918 egress and ingress checks as well as the general lack of reverse path forwarding checks that could, and should be implemented at network boundaries. There are a wealth of single packet UDP exploits that can be delivered from spoofed source addresses, including buffer overruns and DNS Infrastructure attacks.

See: <http://www.ngssoftware.com/advisories/mssql-udp.txt>

TCP with sequence number prediction

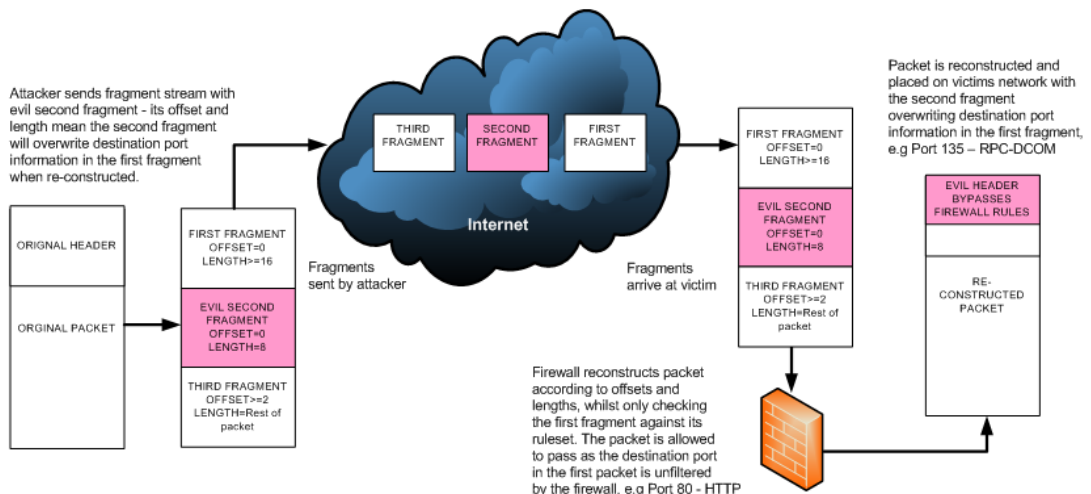
One of the first attacks against the TCP/IP protocol suite, described by Robert Tappan Morris in 1985, was first used by hacker Kevin Mitnick against Tsutomu Shimomura, a top IT security expert. TCP, unlike UDP, is a connection based protocol that uses sequence and acknowledgement numbers to maintain connection state when two parties are communicating. Predictable initial sequence numbers allow the attacker to inject spoofed packets into a TCP stream, as most other higher layer protocols 'trust' TCP, they do not perform their own connection state checking or data integrity checks. This attack is known to be hard to perform, however underground tools to make the job easier are becoming increasingly available. We have noticed recently that new and common, application specific devices (cheap home routers, webcams, VoIP phones, etc) are generating predictable initial sequence numbers.

See: <http://lcamtuf.coredump.cx/newtcp/>

Fragmented Packet Handling

Attacks like the teardrop attack used tiny fragmented packets to circumvent firewall rules and crash devices. Some firewalls do not inspect individual packet fragments; they only examine the initial packet that contains the IP header. Other fragmented packet attacks cause many modern systems to stop functioning (DoS), a recent example affecting multiple vendors is referenced below:

See: <http://xforce.iss.net/xforce/xfdb/17561>



Source-Routing

Combined with sequence number prediction, but not always necessary, source-routing allows the attacker to actually communicate with the application being attacked and receive data back, even though the packets used for the attack have spoofed source addresses. Source-routing is used legitimately by network engineers to analyse connectivity between different points in a network with multiple routers and subnets without complexity. Some operating systems may also crash when receiving malformed source-routed packets. Most networks block source-routed packets on network

borders, however it is common practice to allow source-routing within an administrative domain. The attacker may compromise a random customer on the same ISP as the target organisation and launch a successful attack using source-routing from there.

See: <https://www.auscert.org.au/render.html?it=159>

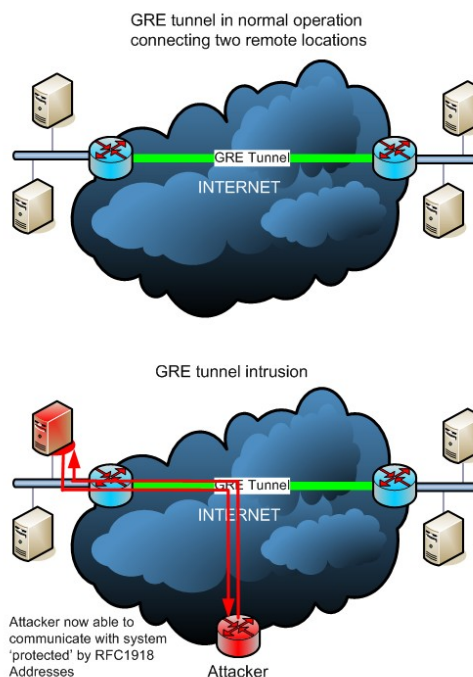
See: <http://isc.sans.org/diary.php?storyid=1410&rss>

GRE Tunnel Remote Sniffing and Intrusion

GRE Tunnels are often used by service providers and organisations to connect networks together during topology changes and to provide quick link layer connectivity to remote netblocks. They are also used by customers to connect branch offices together in a virtual LAN.

If an organisation's router or upstream ISP router carrying the organisations traffic is compromised, it is possible for the attacker to sniff and intercept any data that is being forwarded through it using GRE tunnels from any remote location across the internet. The attacker creates a GRE tunnel on the router pointing to their own, remote GRE capable device. The attacker then applies rulesets on the compromised router to select the required traffic for sniffing. This traffic is routed to the attacker, who can then sniff or change the data before routing it back to the compromised router. With enough bandwidth and detailed, specific rulesets, this attack is almost invisible to the victim especially if the attacker has a chain of tunnels through compromised devices.

GRE Intrusion does not rely on the attacker having access to tunnel endpoints; instead spoofed packets are used to trick end systems into sending data to the attacker. This attack can be very stealthy if the attacker has access to a fast internet connection. GRE tunnels are often ignored, even if unsecured 'if it works, don't fix it'.



See: <http://www.phenoelit.de/irpas/gre.pdf>

Why is this happening?

We have overviewed some of the types of attack we have seen in the distant past which we are now seeing again. What's more worrying is that these attacks are now being combined with many of the newer types of attack making them even more difficult to detect and defend against.

The re-emergence of the attacks outlined above is due to a number of combined factors. Technology is evolving rapidly with new communication protocols such as XMPP, RTP and H.323, the ever increasing spread of the wireless network and new network devices like VoIP exchanges and VoIP phones. In some cases it has resulted in network operators being side-tracked by the need to keep up with this pace of change, but in many cases it has resulted in a conscious decision by network operators to 'relax' configuration settings to enable this evolution to take place. This may be due to limited IT resources, but if you consider the same actions in a personal scenario, it is very obviously wrong; just because there is a chance that a hacker could gain access to your home network to steal personal banking information, you wouldn't just concentrate on securing your LAN and begin to leave your front door open!

Also with the increasing complexity of the latest attacks we are seeing in the marketplace such as this recent example from the North American Network Operators Group (NANOG) mailing list, there is the incorrect and dangerous assumption that these old attacks are rated as insignificant and the perceived importance of them is extremely low. However, as can be seen from this example, combined attacks make use of modern and old techniques simultaneously:

"It reads almost like a mystery novel, involving cloaking, promiscuous interfaces, stolen IP addresses, and tunnelling. It gets a little tricky, so follow the bouncing ball

- *The spammer obtains a dedicated server at the victim's service provider. The server shares a subnet with other customers;*
- *A spamware daemon is installed on the dedicated server, to keep the network interface in promiscuous mode;*
- *The daemon determines which IP addresses on the local subnet are not in use. It also determines the addresses of the network routers. One or more unused IP addresses are commandeered for use by the spammer;*
- *The perpetrated server sends unrequested ARP responses to only the gateway routers, so that the routers never have to ask for a layer-3 to layer-2 association – it's always in the ARP cache of the routers. Nobody else sees this traffic in an EtherSwitch fabric, so ARPWATCH and its kin are defeated. Pings and traceroutes also fail with "host unreachable.". The daemon then only has to watch on the NIC, in promiscuous mode, for TCP packets to the hijacked address on port 80, and pass them down the tunnel to the remote Web server.*
- *Finally, GRE and IPIP tunnelling is used to connect the stolen IP addresses to the spammer's real servers hosted elsewhere."*

An incredibly complex mix of techniques used to gain access, which is very difficult to follow, let alone detect and remediate against!

Investment in the IT security area is also increasing rapidly, meaning that up-to-date setups and configurations, correctly configured firewalls and the implementation of Intrusion Detection and Prevention Systems are becoming more common. The issue here is that the rate of investment is different for every sector, the financial sector being the most heavily invested in, due to its obvious appeal to hackers. This has meant that other sectors are becoming more attractive to hackers, not only for the prospect of direct financial gain from the targets themselves, but also to be used as staging points

for attacks on other organisations to hide the true identity of the attacker. Basic network scanning leaves these other sectors susceptible to speculative attacks.

That brings us to looking at the nature and motives behind the attacks. The complex attack we reviewed a couple of paragraphs above could be attributed to the thrill of pushing the boundaries of hacking; something to impress fellow black-hats. However, the hacking landscape has also been changing over the last couple of years. There are an increasing number of 'organised' hacking groups seeing 'hacking as a business'. They don't care how they gain access to a network because their motives reside firmly with financial gain. Any infiltration will suffice; it doesn't have to impress any of their counterparts. This is far more alarming.

Conclusion

Organisations, if they haven't already, need to look at investing in a long term Information Security strategy. The likeliness of 'low-hanging-fruit' attacks through speculative scanning is increasing and as other organisations invest in this area, that likelihood only increases further. When an organisation begins the process of reviewing their strategic requirements they should look at their business in terms of a number of variables, each of which increases their risk of attack:

- *Number of locations – network map associated with each*
- *Number of staff – remote workers*
- *Different types of technology used – VoIP, VPN, FTP, Wireless networking etc.*
- *Sector – is the industry an attractive target, what are the possible motives?*
- *Level of staff training – are our staff keeping in security in mind?*
- *Level of current Information Security*

IT resource is kept busy ensuring that the business can operate on a day to day basis through its business applications. That is seen as justified resource allocation since it adds to an organisations bottom line. Information Security however, does not add to the bottom line and allocating any more time than the necessary minimum is seen as a waste. This can be a dangerous line to follow. From the type of business risk assessment outlined above, organisations will be able to establish a robust business case outlining the required level of Information Security investment and the justification behind it. The strategy established should involve constant monitoring and regular audits, and most importantly it should be cumulative and comprehensive in its scope.

The overriding message that comes out of this for any organisation is not to be complacent where Information Security is concerned. 'Hacking as a business', means that the easier a company makes it for a hacker to gain access, the better from their point of view. Hackers have recognised the opportunity to dust down some old techniques, and they will make the most of it.

About SureCloud

SureCloud is a market leading provider of Software-as-a-Service (SaaS) Information Security Management solutions and professional services. Our modular application suite covers Vulnerability Management, Compliance Management, Asset Management and Risk Management – providing a cost effective way for our clients to tailor security solutions to meet their individual security needs.



Furthermore, we tightly integrate professional services, such as penetration testing, with our SaaS applications, providing our clients with full control of the entire information security life-cycle.