IMMUNITY

Going Against The Gradient

Dave Aitel
December 2007

There's a natural force in information security technology. Like gravity, it can give someone on the wrong side of it a hard slog, and then a long fall. Over time, you'll get less and less for your investment. The amazing thing is that so many product spaces in information security are on the wrong side of the equation. These products are in for a radical and sometimes devastating change.

Some products have been struggling to maintain technical relevance even as their market share grows. Anti-Virus is one of them. On one hand, signatures are great, because they tell you exactly what sort of problem you're having, and how to fix it. On the other hand, when you get to the point where you have to write a custom Javascript engine to pre-parse all the data coming in from the web browser, you're in trouble - and adding a quarter million signatures a year to your database is horribly painful just in terms of bandwidth, both yours and your customers'. From the attacker's perspective, it is a thousand times easier to hide from anti-virus than it is for the anti-virus companies to write protection against you. Projects such as VirusTotal show you how horribly inconsistent anti-virus coverage is even for things they know about. For 0day or targeted attacks, anti-virus just doesn't have a chance.

IDS and IPS have the same problem but with additional issues. Network protocol complexity increases exponentially as each protocol can be wrapped in other protocols. This requires that IDS stores more and more state, using more and more memory and CPU. Another natural enemy of IDS is encryption. Many protocols support some level of encryption by default now. If a network administrator wants to take advantage of IPSEC across their enterprise, they've just completely blinded their IDS. IDS companies claim that with sufficient "tuning" you can get a lot of value out of their products because you've reduced the false positive rate. This is less and less true as time goes on. If the answer to false positives from your IDS company is to give the IDS itself a giant picture of the network it is protecting and have it emulate all the potential targets with every packet it parses, then you've got a problem.

There's another important actor working against many software products: Microsoft. Aside from developing a direct competitor to the Anti-Virus products themselves, Microsoft wants to lock everyone out of the Vista and Windows 2008 kernels. This would put a lot of products out of business. Aside from legal issues, there's nothing technologically preventing Microsoft from doing this. Many companies are going to find themselves locked down into a smaller and smaller Kernel API as time goes on, while fighting a larger and larger base of malware more and more ineffectively.

The lesson learned here is that sniffing the network or writing a Windows kernel plugin is not the answer to your problems. Why is the emerging Anti-Data-Leakage industry having such big problems? Because they're going against the technology gradient by implementing both sniffers and kernel-based agents.

Many products, in particular hard drive forensics, also have to fight the Digital Rights Management industry. DRM is heavily reliant on locking data to a particular machine. Various motherboards now contain chips with built in encryption/decryption and key storage specifically for making it possible to encrypt data that is useless to non-authorized processes. While trojans don't currently take advantage of this, as the TPM technology becomes more widespread and popular, expect them to lock themselves to each machine they infect, making disk images useless. Newer forensics efforts concentrate on having a executable running on

the machine and grabbing all that machine's memory, something Microsoft's trusted computing work specifically protects against.

These days sales of many products are driven by compliance issues, and hence, the lowest cost vendor invariably wins. If you're wondering about this, just turn around and ask your million dollars worth of IDS equipment and personnel when the last time they caught a hacker was. Encryption, network protocol complexity, and continued attacker innovation have rendered your existing security arsenal useless. This year's question is: What are you going to do about it?