The Significance of the "Nitro" Attacks

blog.trendmicro.com/trendlabs-security-intelligence/the-significance-of-the-nitro-attacks/

October 31, 2011

This report illustrates some of the key findings in our latest white paper, Trends in Targeted Attacks.

By: Trend Micro October 31, 2011 Read time: (words)

A recent report by Symantec documented a campaign of targeted malware attacks that began as early as April 2011 and continued up to October 2011. During this time, the attackers managed to compromise at least 100 computers around the world. This report illustrates some of the key findings in our latest white paper, Trends in Targeted Attacks.

Targeted Campaigns

Targeted malware attacks are rarely isolated events. It is more useful to think of them as campaigns – a series of failed and successful attempts to compromise targets over a period of time. An attacker's prior knowledge of the victim, possibly from a previously successful attack, affects the level of specificity associated with a single attack in a malware campaign. In this case, the attackers used messages with an IT security theme that appeared rather generic but were customized for various targets. The download link in the email messages was made to appear as if it were pointing to the target’s own website. Often, this less-specific level of targeting focuses on communities of interest and is aimed at acquiring information to be used in a future, more precise attack.

Moreover, there is generally a diversity of targets. In this case, the Nitro attackers targeted a concentration of chemical companies but also targeted human rights NGOs, motor companies and defense contractors.

Human Interaction

The backdoor used in the Nitro campaign is known as Poison Ivy. It is a freely available Trojan that provides an attacker with full, "real-time" access to a compromised computer. One often overlooked component of targeted malware attacks is the reliance on real time human interaction. This distinguishes them from automated botnets. When the Poison Ivy backdoor connects to the attackers command and control infrastructure there is a human at the other end that can begin exploring the compromised computer and the network to which it belongs. This attacker can steal information, install additional malware and compromise other machines on the same network. Most importantly, the human on the other end of the Poison Ivy Trojan can react to defensive measures taken by the victim.

Segmented Infrastructure

Attackers need to deploy command and control (C&C) infrastructure in order to maintain connectivity to the computers they compromise. The attackers sometimes maintain distinct sets of C&C infrastructure making it difficult to uncover the full extent of their operations. Using the initial malware samples, domains and IP addresses provided by Symantec, we were able to map out three distinct sets of command and control infrastructure. The first set of command and control infrastructure contains three domains provided by dynamic DNS services. Attackers often use dynamic DNS services in conjunction with RATs, such as Poison Ivy. These services make it easy for the attackers to update their C&C domains to new IP addresses thus maintaining consistent connectivity with the compromised computers.

Click for larger view

The second set of C&C infrastructure centers around three domains which all resolved to the same IP address. The C&C domain, *domain.rm6.org* was also used in an attack. on the UK government in August 2011.

Click for larger view

The third set centers on the domain *antivirus-groups.com* and the IP address *204.74.215.58* which Symantec has associated with a specific actor which they've codenamed "Covert Grove".

Click for larger view

This segmented infrastructure allows the same set of attackers to target different potential victims without having all the attacks linked together. Without additional information, it can be difficult to link together the full scope of targeted malware campaigns. This illustrates how important threat intelligence is to defensive strategies. Here are some examples of MD5s connecting to the Nitro infrastructure:

- 37f70717f549f1938e5785527e56978d
- 5d075e9536c5494745135c1176981c96
- 64a4ad90a55e7b6c30c46135435f50a2
- 6e99585c3fbd4f3a55bd8f604cb35f38
- 70fcb3446fce23b18d9a12b2ed911e52
- 76000c77ea9a214f5b2ae8cc387809db
- 87aeec7f7c4ec1b6dc5e6c39b28d8273
- 8d36fd85d9c7d1f4bb170a28cc23498a
- a98d2c90b9494fc885c7cd35d43666ea
- c128c40bd8acb282288e8138352ce4e1
- 841ec2dec944964fc54786a1167713ff
- 22f77c113cc6d43d8c12ed3c9fb39825
- 6f6d6a848f87fbf26f71549d73da61f4
- b2b9702164512a92733939343275245b
- 2173b43a66070aadf052ab66dd6933ce
- f18c7639dbb8644c4bca179243ee2a99
- 9ff1e8e227e1be3dbfc55f17d2e97df8
- 31346e5b39ddb095d76071ac86da4c2e
- 20baa1cbacdab191c717f4ef5626de93
- ffa73b9f9e650f50b8568a647a9a35cf
- 070d1e5c9299afa47df25e63572a3ae8
- d558e1069a0f3f61fedcf58a0c1995fe
- 27103c6c9a80b6cf23789e2f51a846eb
- 2ffe59a6a047b2333a1f3eb58753f3bc
- 0f54a9757f1a2fef2b04b776714a7546
- c2864aff6360feb36f2ff6a6c634ddb4
- cca3af36dff79b27de093a71396afb8d
- 4a35488762f70170dc0d3f46f94a7bcb
- 3037049411db0453c91e60393a248be2
- dd5715cb3b0cdddbe131f03cc08f0f57
- 4fd6453a606e17e5efb166ad80eba5e0
- 091457444b7e7899c242c5125ddc0571
- 6e99585c3fbd4f3a55bd8f604cb35f38
- 07e266f7fb3c36a1f3a5c5d2d229a478
- 17e7022496d8092d3ca76ae9524a7260
- 2f37912e7cb6e5c478e6dc3d0e381a24
- 5d075e9536c5494745135c1176981c96

- 76000c77ea9a214f5b2ae8cc387809db
- a98d2c90b9494fc885c7cd35d43666ea
- c128c40bd8acb282288e8138352ce4e1
- cab66da82594ff5266ac8dd89e3d1539
- 70fcb3446fce23b18d9a12b2ed911e52
- c53c93a445d751387eb167e5a2b901da
- dd5715cb3b0cdddbe131f03cc08f0f57
- 0f54a9757f1a2fef2b04b776714a7546
- 37f70717f549f1938e5785527e56978d
- 31346e5b39ddb095d76071ac86da4c2e
- 330ddac1f605ff8abf60880c584ed797
- 457a2a8d0784e9fc8e49f6ef60f7f29e
- 87aeec7f7c4ec1b6dc5e6c39b28d8273
- 8d36fd85d9c7d1f4bb170a28cc23498a
- de7e293aa9c4d849dc080f3e87573b24
- 64a4ad90a55e7b6c30c46135435f50a2

Defensive strategies can be dramatically improved by understanding how targeted attacks work as well as trends in the tools, tactics and procedures of the perpetrators. Since such attacks focus on the acquisition of sensitive data, strategies that focus on protecting the data itself, wherever it resides, are extremely important components of defense. By effectively using threat intelligence derived from external and internal sources combined with context-aware data protection and security tools that empower and inform human analysts, organizations are better positioned to detect and mitigate targeted attacks.