The Current State of Ransomware

The Current State of Ransomware

In the past year or two, one of our most popular technical topics, for all the wrong reasons, has been ransomware.
Ransomware, as we're sure you know, is the punch-in-the-face malware that scrambles your files, sends the only copy of the decryption key to the crooks, and then offers to sell the key back to you.
Even Linux has ransomware these days, although fortunately we've only seen one serious attempt at Linux-based extortion so far, presuambly because cybercriminals haven't yet figured out how to make money in that part of the IT ecosystem.
Let's hope it stays that way for Linux sysadmins, because the crooks are still attacking Windows users heavily, and are still raking in lots of ill-gotten gains.

THE CRYPTOLOCKER YEARS
Two years ago, one strain of ransomware known as CryptoLocker dominated the demanding-money-with-menaces malware scene.
The US Department of Justice (DoJ) suggested that the crew behind CryptoLocker raked in $27,000,000 in September and October 2013 alone, in the first two months that the malware was widely reported.
And a 2014 survey by the University of Kent in England estimated that 1 in 30 British computer users had been hit by CryptoLocker, and that 40% of those coughed up, paying hundreds of dollars each in blackmail money to recover their data.
But in mid-2014, the DoJ co-ordinated a multi-country takedown of a notorious botnet called Gameover Zeus that targeted victims while they were doing online banking.
And, would you believe it: while the cops were raiding the Gameover servers, they came across the CryptoLocker infrastructure as well, and took down those servers at the same time, pulling off a neat double play.
CryptoLocker doesn't start its data scrambling until after it has called home for an encryption key, so killing its servers pretty much neutralised the warhead of the malware: it would get right to the very brink of detonation and then freeze, waiting for data that never came.
But any celebration about the damage done to the ransomware scene as a whole was short-lived.

RANSOMWARE REDUX
Cybercrime, if you will tolerate a clumsy metaphor, abhors a vacuum, and new ransomware soon appeared to fill the multi-million-dollar void left by the demise of CryptoLocker.
CryptoWall, and its close derivative CryptoDefense, were early pretenders to CryptoLocker's throne, but many others have appeared, too.
Threats like TorrentLocker, CTB-Locker and TeslaCrypt are big names these days, joined by other intriguing threats such as VirLock, ThreatFinder (an ironic name, considering that it is itself the threat) and CrypVault.

WHAT TO DO?
When it comes to malware of this sort, the dictum "know your enemy" is worth remembering.
With this in mind, James Wyke and Anand Ajjan, who are Senior Threat Researchers in SophosLabs, have recently published a thorough and well-written paper entitled The Current State of Ransomware.
This paper is a highly-recommended read – and it's a free download, no registration required.
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en

You'll learn about the history of ransomware, the latest threats, how they work, and what you can do to defend yourself.
Great stuff from SophosLabs!

Réagissez à cet article

Source : *The Current State of Ransomware – a new paper from SophosLabs |*