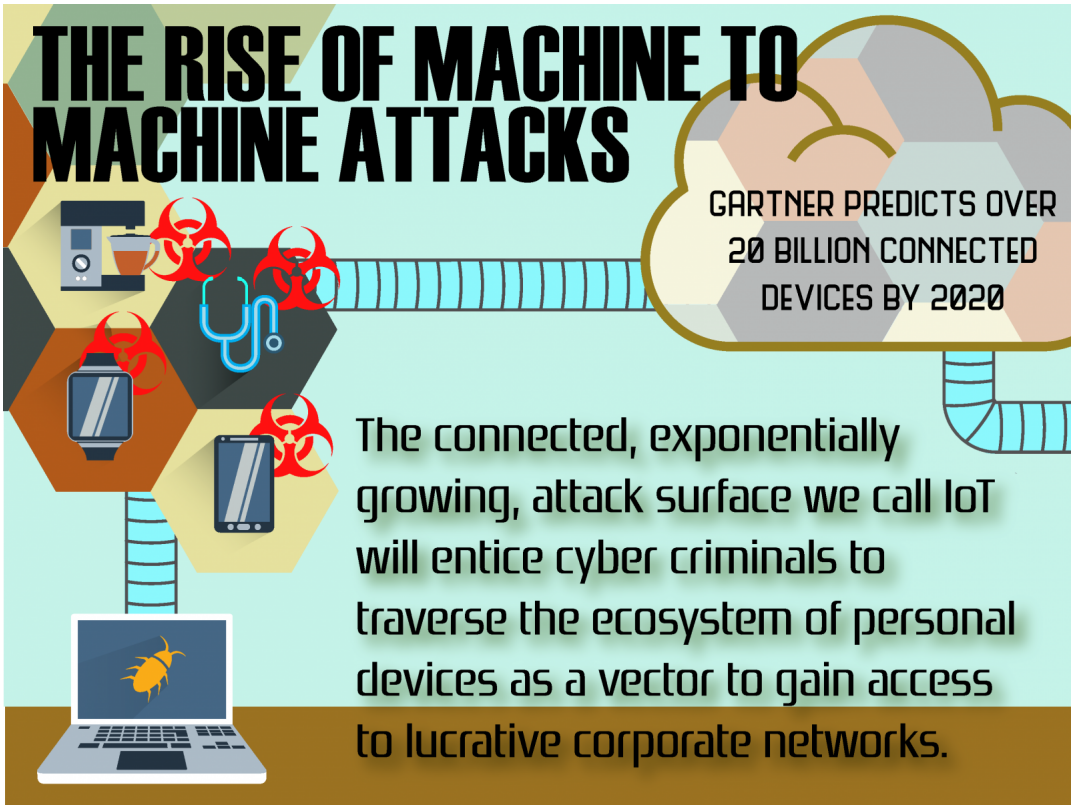
The Top 5 Threat Predictions For 2016 From FortiGuard Labs

by **Derek Manky (/author/derek-manky)** | November 24, 2015 | Category: Industry Trends & News (/category/industry-trends-news)

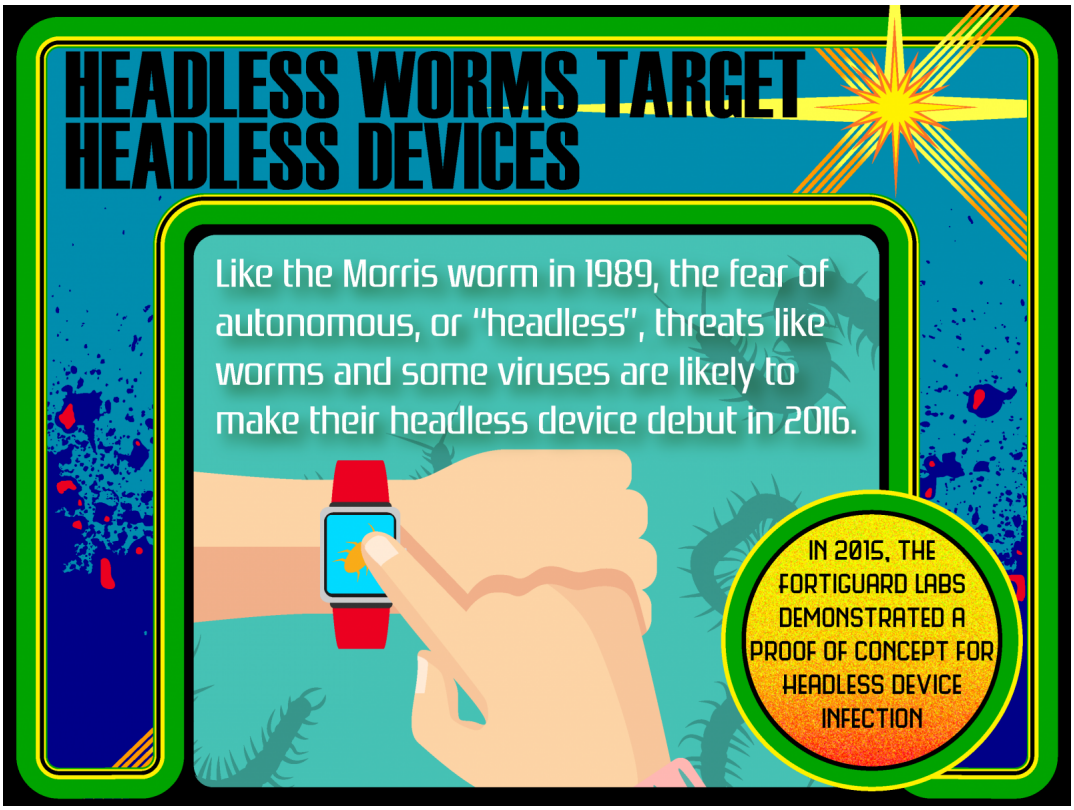
It's an annual tradition that security vendors and pundits alike can't resist: threat predictions for the coming year. However, this is much more than an exercise in crystal ba gazing. Vendors need to accurately predict changes in the threat landscape to design products that effectively address emerging issues. Organizations need to plan appro defenses and deploy countermeasures before a novel attack occurs instead of trying to pick up the pieces afterwards.

So what are the trends beyond the buzzwords? Fortinet's FortiGuard Labs has picked the top five emerging threats (http://www.fortinet.com/resource_center/whitepapers predictions-evolving-threat-landscape.html) that will challenge our defenses and push vendors to develop novel solutions that protect customers from increasingly savvy cybercriminals, more intelligent malware, and more determined state actors.



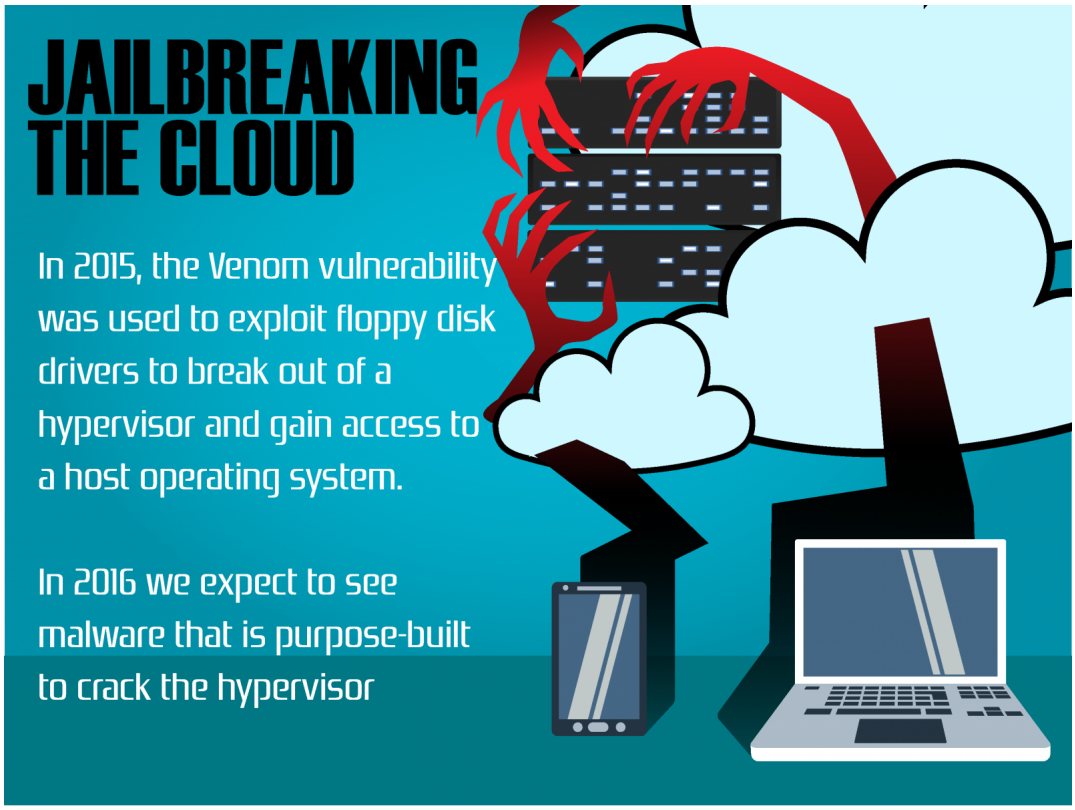
No, this isn't the title of a bad sci-fi movie. 2015 saw a number of proofs of concept and active attacks involving connected "headless devices" – the so-called Internet of T Malware that infects Point of Sale devices, for example, is now in Japan's top 10 list of malware in the wild, while researchers made headlines by compromising and contr connected vehicle in motion (http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/).

In 2016, though, we expect to see further development of exploits and malware that target trusted communication protocols and APIs like Bluetooth, Zigbee, and others commonly used by IoT devices. More importantly, IoT will become central to "land and expand" attacks. Hackers will take advantage of vulnerabilities in everything from sr home devices to wearables to compromise corporate-issued devices or corporate networks. As the attack surface for IoT grows dramatically, so do the opportunities to propagate malware among the devices, many of which may find their way onto corporate networks or connect to repositories of personal data.



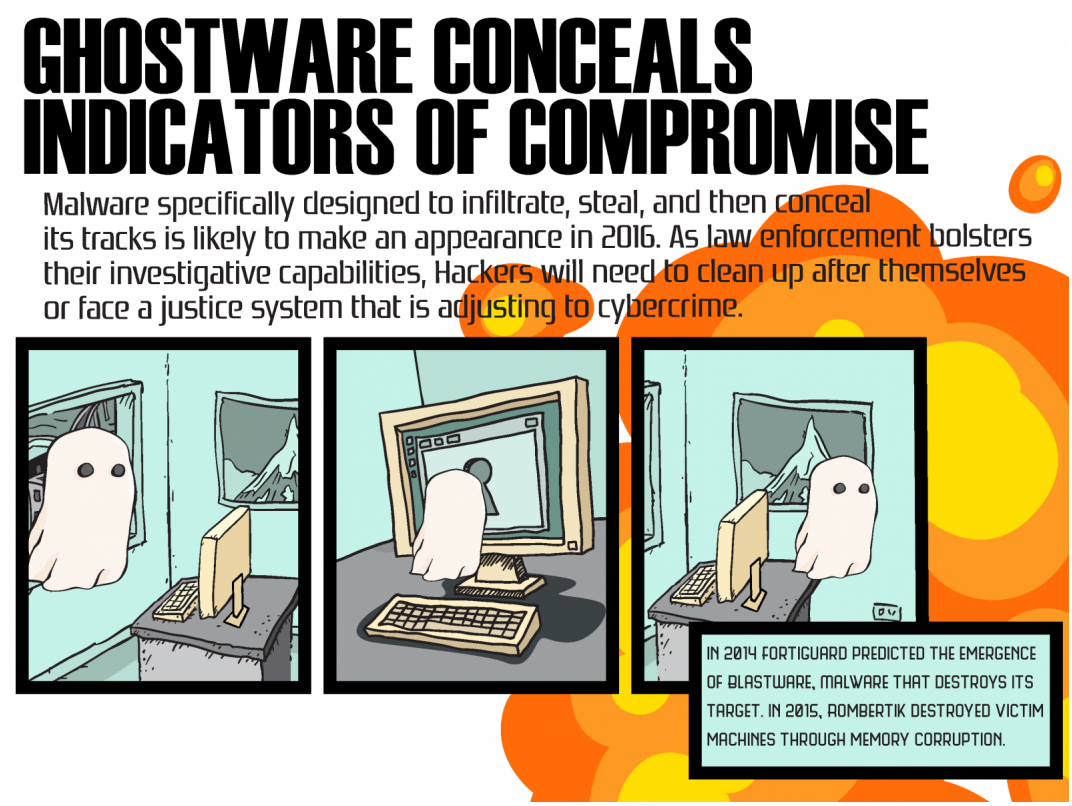
Yes, the sci-fi allusions continue, but for good reason: IoT will not just give rise to larger attack surfaces with more exploitable vulnerabilities but also to new targets for des malware. Consider the Morris worm, which hit Unix-based operating systems in 1989. It infected roughly 10% of connected Unix machines (at the time, a mere 6000 serve workstations). Damage estimates ran into the millions from this worm. Now consider that Gartner predicts that there will be more than 20 billion IoT devices by 2020. You the math, but the potential damage caused by "headless worms" that could disable these machines is staggering.

FortiGuard researchers and others have already demonstrated that it is possible to infect headless devices with small amounts of code that can propagate and persist. Wo and viruses that can propagate from device to device are just around the corner.



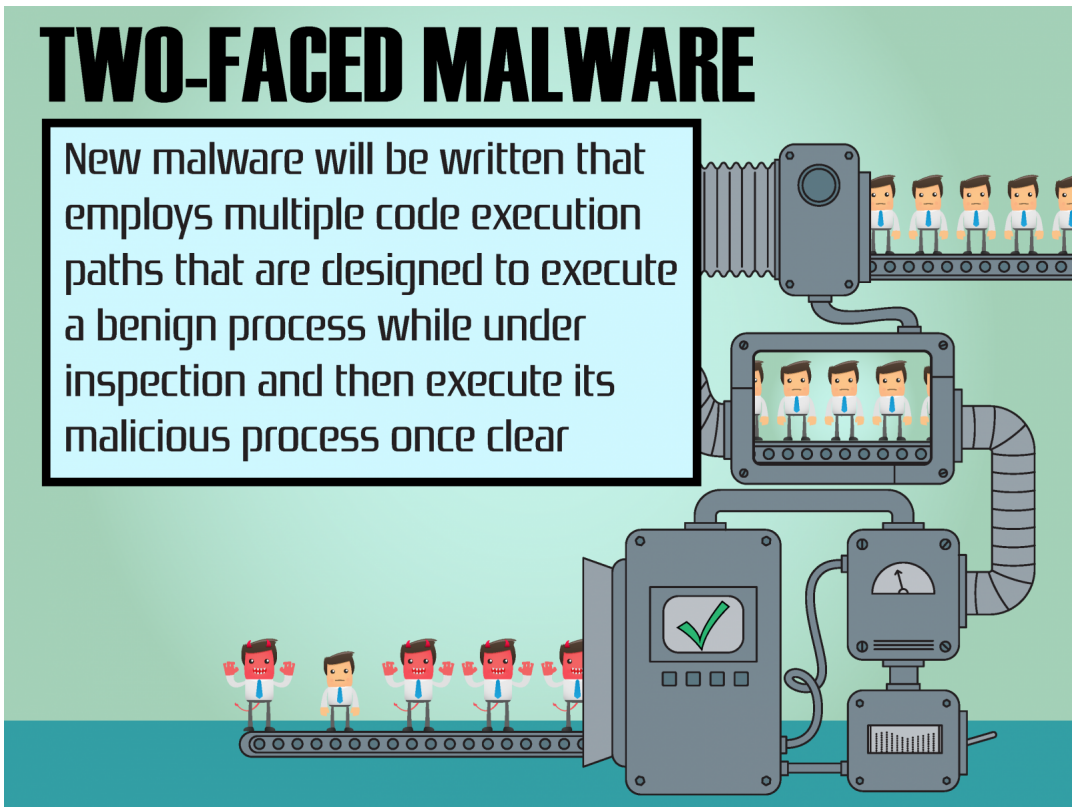
Just this year, a decade-old vulnerability known as Venom captured media attention when it became clear that it could use floppy disk drivers on virtualized systems to bre of the hypervisor and access the host operating system. As adoption of cloud and virtualization technologies continues to increase, we expect attackers to develop malwa seek out vulnerabilities that can further compromise host systems. It's a short step then, to additional corporate assets and the larger network in virtualized and private/hyb cloud environments.

Beyond attacks on virtualized systems, though, attacks on both public and private cloud-based systems are increasingly likely. The prevalence of mobile applications (agai from public and corporate app stores) make mobile devices potential vectors for remote attacks on cloud-based applications and virtualized systems.



In 2014, we predicted the emergence of “blastware”, malware designed to destroy both itself and the host system if it was detected by antivirus software. Rombertik, thou somewhat overblown in the media, gave the first hint of what this kind of software could do to infected systems. We expect blastware to continue to surface, especially in of hacktivism and state-sponsored cybercrime.

However, ghostware takes this concept further. Whereas blastware leaves the ultimate indicator of compromise (a crashed or disabled system), ghostware is designed to extricate data and then erase indicators of compromise before it can be detected, making it very difficult for organizations to track the extent of data loss associated with a attack.



If evading detection after infection is the name of the game for ghostware, two-faced malware is all about evading detection at the outset, even under inspection by advan

sandboxing techniques. Sandboxes are designed to observe the behavior of potentially malicious files at runtime, detecting software that may not be flagged by traditional antivirus. If malware is developed, though, that behaves normally while under inspection and then delivers a malicious payload once it has been passed by the sandbox, th prove quite challenging to detect.

More significantly, this two-faced malware may be flagged as safe by the sandbox and then reported back to vendors' threat intelligence systems so they aren't inspected future, compounding the challenges to vendors and organizations associated with this type of malware.

The bottom line for vendors is that malware authors are getting savvier while attackers are taking advantage of growing attack surfaces. For organizations, selecting vendo can keep up with these new threats will be critical to staying on top of malware and preventing data loss and system destruction in 2016.

Click here (http://www.fortinet.com/resource_center/whitepapers/2016-predictions-evolving-threat-landscape.html) to download the full report from FortiGuard Labs.

by **Derek Manky (/author/derek-manky)** | November 24, 2015 | Category: Industry Trends & News (/category/industry-trends-news)

Tags: fortiguard labs (/tag/fortiguard-labs) | predictions (/tag/predictions)

FortiGuard Labs on the Web

Twitter (http://www.twitter.com/fortiguardlabs) Facebook (https://www.faceb
LinkedIn (http://www.linkedin.com/groups?gid=1321377&trk=hb_side_g) Youtube (http://www.youtub

Monthly Archives

November 2015 (/2015/11)	11
October 2015 (/2015/10)	19
September 2015 (/2015/09)	11
August 2015 (/2015/08)	17
July 2015 (/2015/07)	22
June 2015 (/2015/06)	18
May 2015 (/2015/05)	16
April 2015 (/2015/04)	34
March 2015 (/2015/03)	17
February 2015 (/2015/02)	11
January 2015 (/2015/01)	16
December 2014 (/2014/12)	7
November 2014 (/2014/11)	19
October 2014 (/2014/10)	16

September 2014 (/2014/09)	**11**
August 2014 (/2014/08)	**11**
July 2014 (/2014/07)	**20**
June 2014 (/2014/06)	**21**
May 2014 (/2014/05)	**19**
April 2014 (/2014/04)	**16**
March 2014 (/2014/03)	**20**
February 2014 (/2014/02)	**15**
January 2014 (/2014/01)	**25**
December 2013 (/2013/12)	**10**
November 2013 (/2013/11)	**15**
October 2013 (/2013/10)	**19**
September 2013 (/2013/09)	**19**
August 2013 (/2013/08)	**14**
July 2013 (/2013/07)	**14**
June 2013 (/2013/06)	**2**
April 2013 (/2013/04)	**1**
March 2013 (/2013/03)	**12**
February 2013 (/2013/02)	**11**
January 2013 (/2013/01)	**12**
December 2012 (/2012/12)	**8**
November 2012 (/2012/11)	**7**
October 2012 (/2012/10)	**4**
September 2012 (/2012/09)	**6**
August 2012 (/2012/08)	**7**
July 2012 (/2012/07)	**62**
June 2012 (/2012/06)	**17**
May 2012 (/2012/05)	**14**
April 2012 (/2012/04)	**15**
March 2012 (/2012/03)	**14**
February 2012 (/2012/02)	**11**
January 2012 (/2012/01)	**6**
December 2011 (/2011/12)	**4**
November 2011 (/2011/11)	**6**
October 2011 (/2011/10)	**11**
September 2011 (/2011/09)	**2**
August 2011 (/2011/08)	**2**
July 2011 (/2011/07)	**4**
June 2011 (/2011/06)	**6**
May 2011 (/2011/05)	**6**
April 2011 (/2011/04)	**5**
March 2011 (/2011/03)	**7**

February 2011 (/2011/02)	**5**
January 2011 (/2011/01)	**7**
December 2010 (/2010/12)	**8**
November 2010 (/2010/11)	**11**
October 2010 (/2010/10)	**3**
September 2010 (/2010/09)	**8**
August 2010 (/2010/08)	**4**
July 2010 (/2010/07)	**9**
June 2010 (/2010/06)	**9**
May 2010 (/2010/05)	**9**
April 2010 (/2010/04)	**6**
March 2010 (/2010/03)	**8**
February 2010 (/2010/02)	**6**
January 2010 (/2010/01)	**9**
December 2009 (/2009/12)	**8**
November 2009 (/2009/11)	**6**
October 2009 (/2009/10)	**6**
September 2009 (/2009/09)	**8**
August 2009 (/2009/08)	**5**
July 2009 (/2009/07)	**8**
June 2009 (/2009/06)	**7**
May 2009 (/2009/05)	**4**
April 2009 (/2009/04)	**7**
March 2009 (/2009/03)	**9**
February 2009 (/2009/02)	**4**
January 2009 (/2009/01)	**1**