GravityRAT malware takes your system's temperature

virusbulletin.com/blog/2018/04/gravityrat-malware-takes-your-systems-temperature/

Posted by Martijn Grooten on *Apr 27, 2018*

Cisco Talos researchers Warren Mercer and Paul Rascagnères recently discovered and analysed 'GravityRAT', an advanced Remote Access Trojan (RAT) that appears to have been used in targeted attacks against organizations in India. Analysis of this piece of malware gives an interesting insight into the current state of malware development.

The malware is delivered through a malicious *Microsoft Office* document, likely sent via email, which is a common way for both targeted and opportunistic malware to infect devices. The authors appear to have uploaded early versions of the malicious document to *VirusTotal*, to measure the detection of their code by a range of anti-virus products.

In general, using *VirusTotal* in this way gives a malware author only limited insight into whether a piece of malware will be blocked: *VirusTotal* uses static anti-virus scanners and thus uploading a malicious file to the service can only help its author understand whether it will be detected as malicious, not whether the malware will actually be allowed to run. On top of a static detection engine, endpoint security software typically includes various layers of protection that aim to prevent both known and unknown malware from running.

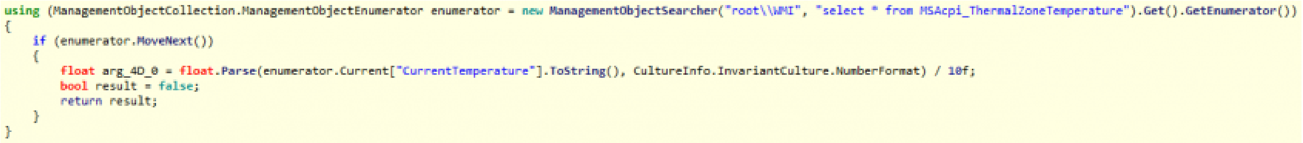
For a malicious document, however, static detection is important in determining whether it will bypass an email security product; if the file is not detected, it is more likely to be able to bypass such security measures – especially if the document is sent only in small quantities, thus not triggering anti-spam detectors in such products.

If the file is opened, and if macros are enabled by the user, the actual payload will be downloaded.

The GravityRAT Remote Access Trojan (or Tool) is noteworthy for the fact that is uses no fewer than seven techniques to detect whether it is running inside a virtual machine.

A lot of today's malware is 'VM-aware', and when it detects that it is being run inside a virtual machine (and is thus likely to be being analysed by a human or a malware-detection sandbox), it either terminates or changes its behaviour. Common techniques for detecting a virtual machine environment include looking for traces of the hypervisor left on the virtual machine, checking the computer name, and checking the number of CPU cores – all of which GravityRAT does.

But it also uses a novel technique where it requests the CPU temperature – a feature not commonly supported by hypervisors. These will then respond 'not supported', thus revealing that the malware is probably not being run on a real machine.



```
using (ManagementObjectCollection.ManagementObjectEnumerator enumerator = new ManagementObjectSearcher("root\\WMI", "select * from MSAcpi_ThermalZoneTemperature").Get().GetEnumerator())
{
    if (enumerator.MoveNext())
    {
        float arg_4D_0 = float.Parse(enumerator.Current["CurrentTemperature"].ToString(), CultureInfo.InvariantCulture.NumberFormat) / 10f;
        bool result = false;
        return result;
    }
}
```

For many years, there has been a continuous cat-and-mouse (cat-and-rat?) game between malware writers and the developers of virtual machines and sandboxes. Analyses like this help the latter update their tools and thus force the malware authors to work even harder.

Warren and Paul spoke at VB2017 last year and will be back at VB2018 in Montreal, to discuss the 'Olympic Destroyer' malware. Registration for VB2018 will open very soon.

Latest posts:

New paper: Collector-stealer: a Russian origin credential and information extractor

In a new paper, F5 researchers Aditya K Sood and Rohit Chaturvedi present a 360 analysis of Collector-stealer, a Russian-origin credential and information extractor.

VB2021 localhost videos available on YouTube

VB has made all VB2021 localhost presentations available on the VB YouTube channel, so you can now watch - and share - any part of the conference freely and without registration.

VB2021 localhost is over, but the content is still available to view!

VB2021 localhost - VB's second virtual conference - took place last week, but you can still watch all the presentations.

VB2021 localhost call for last-minute papers

The call for last-minute papers for VB2021 localhost is now open. Submit before 20 August to have your paper considered for one of the slots reserved for 'hot' research!

New article: Run your malicious VBA macros anywhere!

Kurt Natvig explains how he recompiled malicious VBA macro code to valid harmless Python 3.x code.