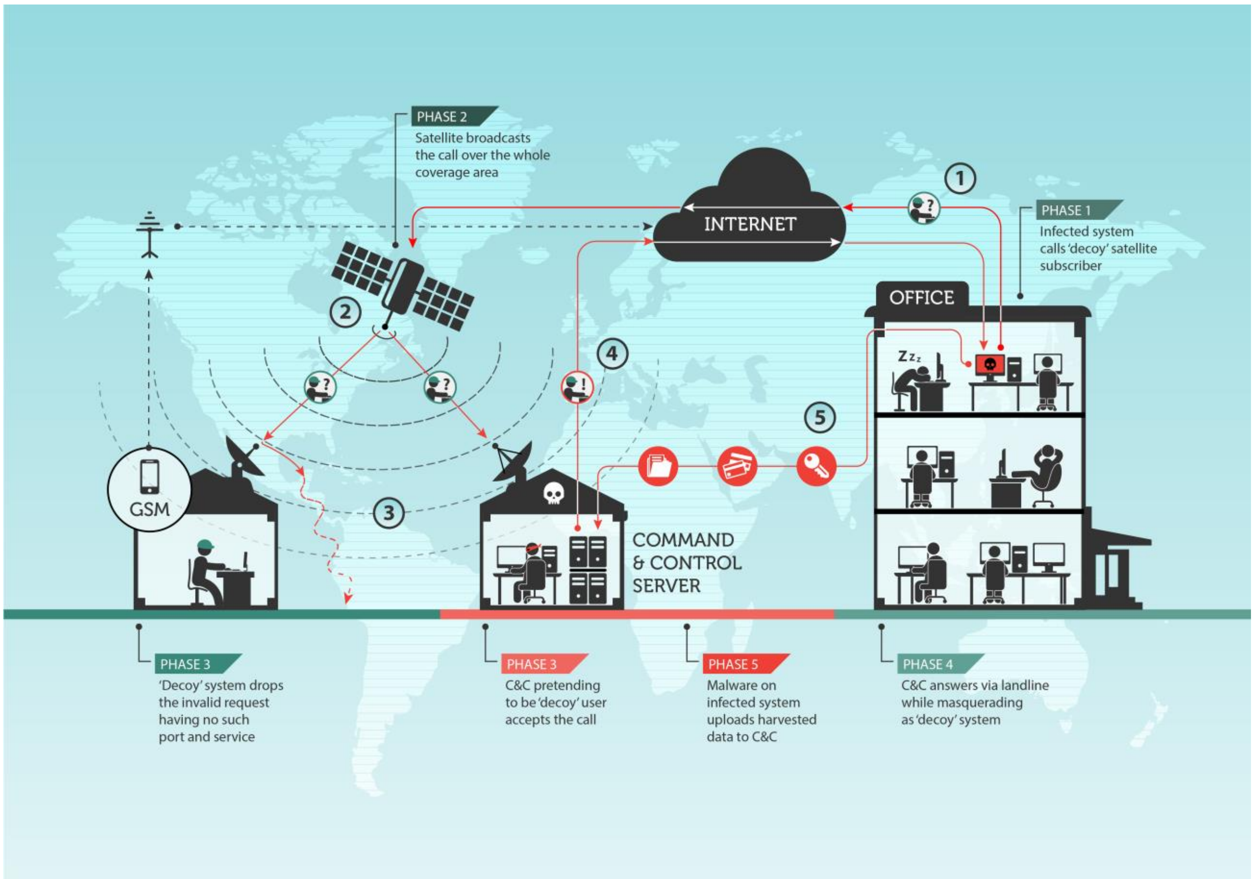
Satellite Turla: still alive and hiding in the sky

Law enforcement agencies, with the help of leading IT security providers, are keen on blocking all the malware Command & Control servers they find. Sometimes, they efficiently shut down massive botnets by putting their controlling structure out of business. But one of the most advanced threat actors is still out there.

One of the reasons for Turla's success, besides the group's obvious professionalism, is their ability to hide the ends – namely, the above-mentioned C&Cs. Research by Kaspersky Lab experts reveals that they're achieving this using a trick known as satlink hijacking – a technique this Russian-speaking group has been using since 2007. It involves exploiting the vulnerability of asynchronous satellite internet connections to sniff traffic, distilling the IP addresses of satellite subscribers. All the attackers need then is to set up their servers with the same IPs, configure these addresses into their malware and, after a successful infection, wait for its call for C&C.

What happens next: the satellite broadcasts the request from an infected machine over the whole area of its coverage. Of course, both attackers and law-abiding subscribers receive this request. But, unlike the attackers' servers, subscriber systems are extremely unlikely to host any services on particular ports – and this traffic is simply dropped without acknowledgement, as this would increase the burden on the thin cellular upstream channel used in such asynchronous data links. After receiving the malware call, the C&C answers via regular fast landline with a spoofed acknowledgement, which appears to be coming from the same hapless satlink subscriber.


PHASE 2
Satellite broadcasts the call over the whole coverage area
INTERNET
1
PHASE 1
Infected system calls 'decoy' satellite subscriber
OFFICE
2
4
5
GSM
3
COMMAND & CONTROL SERVER
PHASE 3
'Decoy' system drops the invalid request having no such port and service
PHASE 3
C&C pretending to be 'decoy' user accepts the call
PHASE 5
Malware on infected system uploads harvested data to C&C
PHASE 4
C&C answers via landline while masquerading as 'decoy' system

This isn't the only trick in Turla's arsenal – there are other mechanisms potential victims should be more worried about. For initial penetration, they use several different methods, including extremely precise waterholing tactics (infecting only victims with IPs hackers are interested in), exploiting several vulnerabilities in visitors' systems. It's worth mentioning that well-known vulnerabilities were actively used, along with zero days, once again proving that automated vulnerability assessment and patch management tools such as those offered by Kaspersky Lab[1] are essential. In the meantime, another security layer found in Kaspersky Endpoint Security for Business - Automatic Exploit Prevention[2] - can block exploits, stopping the attack's development at the very beginning.

Among the other known scenarios used by Turla attackers: spear-phishing emails with Adobe PDF exploits and even fake Flash player or Microsoft Security Essentials installer that are offered for launch with all the persuasiveness of social engineering.

Turla is, unfortunately, just one of many powerful threat actors out there. All use multiple attack techniques, underlining the critical need for true multi-layered security. This not only includes effective endpoint protection (which should include proactive layers such as behavioral mechanisms or Application Control) but also security for other elements of IT infrastructure. Mail security is of particular importance due to the widely used practice of spear-phishing.

In addition, Kaspersky Lab's Intelligence Services may be worth particular consideration. The Data Feeds service provides SIEMs and security solutions with knowledge about watering holes or C&C

[1] Vulnerability Assessment and Patch Management are included in Kaspersky Total Security for Business, Kaspersky Endpoint Security for Business Advanced and Kaspersky Systems Management.

[2] Automatic Exploit Prevention technology is available in all tiers of Kaspersky Endpoint Security for Business and in Kaspersky Security for Virtualization | Light Agent.

servers, which, in accordance with Turla specifics, may prove especially useful. And because thehuman factor is the most exploited vulnerability ever, different levels of Cybersecurity Training for regular employees as well as IT staff is worth considering.

Make no mistake: though Turla's targets are mostly government, military, research and pharmaceutical organizations , your enterprise could still be attacked. Your business contacts with any of these could, in Turla's eyes, make your IT network a stepping stone for attacking the juicier target. You therefore need a comprehensive strategy – and if you are keen on implementing one, the Kaspersky Enterprise Portfolio of products and services could be the answer.

The components of Turla's toolset are detected by Kaspersky Lab's solutions under the following verdicts:

Backdoor.Win32.Turla.cd
Backdoor.Win32.Turla.ce
Backdoor.Win32.Turla.cl
Backdoor.Win32.Turla.ch
Backdoor.Win32.Turla.cj
Backdoor.Win32.Turla.ck
Trojan.Win32.Agent.dne