Emergence of thinking networks

Mike Fahrion, director of product management, B&B Electronics

When examining Flame, the most sophisticated malware that has appeared to date, investigators discovered an interesting feature: Flame can steal and transmit data from computers that have no Internet connections.

Flame does it by using unsuspecting humans for bi-directional data transport. Flame begins the process by copying itself to every digital storage device that it encounters, including USB sticks and external hard drives. When humans hand-carry portable digital storage devices to unconnected PCs and desktops, Flame copies itself into the new computers and starts stealing data. At this point, traditional spyware would have to upload the loot to a remote Internet server. But Flame is a bit more sophisticated. If there's no Ethernet connection Flame just waits for the next external storage device to come along. When one does, Flame copies itself again and brings along a copy of the stolen data. It repeats the process until it finds a computer with an Internet connection, and then it starts transmitting.

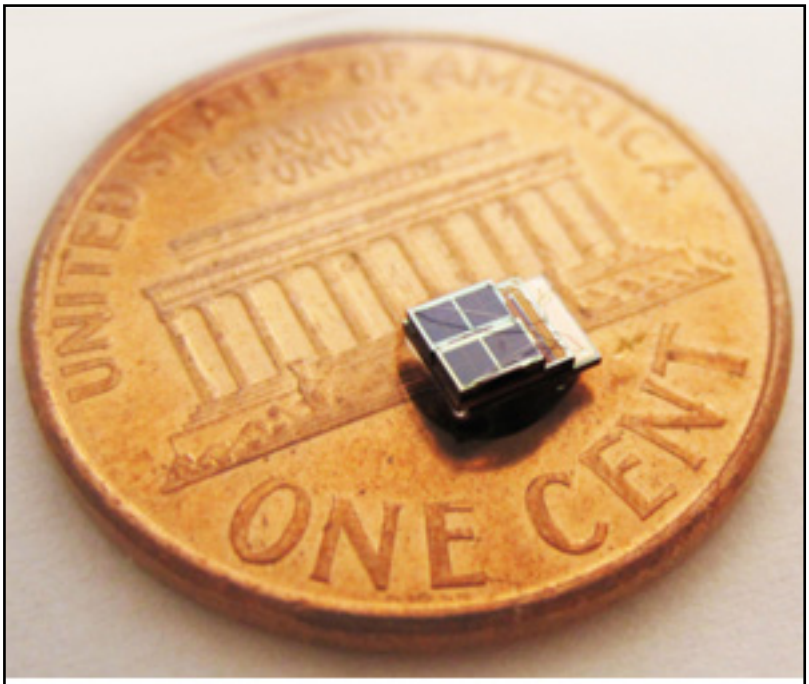

Figure 1. This smart sensor system measures just 9 mm3

Looked at in a certain way, you could say that Flame uses its human data mules as high-latency Ethernet connections. You could also argue that it's an early example of a promising new tool in data communications: Disruption Tolerant Networking (DTN).

The new approach to networking

The old network model assumed that the bulk of a network's intelligence was located in controlling computers. If connections were lost, data would be lost as well. So network designers tried to get as close as possible to what the telcos

famously refer to as “Five Nines” (99.999 percent) uptime. The closer you got to perfection, the harder it was to achieve the next incremental improvement and the more expensive things became.

That model is changing. Downstream devices aren’t necessarily “dumb” anymore. As integrated circuits become steadily smaller and more powerful, and as software becomes more sophisticated, it is becoming easy and cost-effective to distribute localized intelligence all across the network.

The University of Michigan, for example, has developed a low-power, smart sensor system that demonstrates many of the key principles that will be employed in the smarter, “thinking” networks of the future. At just nine cubic millimeters it’s the size of a Vitamin C tablet, but it’s solar powered, it has an internal battery and radio, and it is equipped with its own processor called the Phoenix. (See Figure 1) The processor employs a unique power gating architecture and an extreme sleep mode to achieve ultra-low power consumption. (http://www.engin.umich.edu/newscenter/feature/smallsensor/ [1])

Figure 2. Legacy serial devices are being Ethernet-enabled with Wi-Fi connections using both embeddable and external Wi-Fi Access Points

Smart network nodes like the Phoenix system will provide network designers with opportunities that haven’t been available in the past. Smart nodes will require less bandwidth, for example. They’ll be equipped with situational awareness programming that considers parameters like power, network availability and the status of surrounding nodes to make independent decisions about whether there is any need to log in and report. Smart network nodes will also be able to collect data, time stamp it, log it, and – like Flame -- report the data whenever a network connection becomes available. Even if the network is down for minutes or hours, this Disruption Tolerant Networking model will ensure that data is not lost, thus freeing designers from the need to pursue “Five Nines” uptime.

With their increased efficiency and intelligence, and their ability to hibernate when they have no useful information to report, smart network nodes will require far less power than their “dumb” predecessors. When combined with advances in power harvesting, like the tiny solar panel demonstrated on the Phoenix sensor system, this will give thinking networks the ability to extend the network edge to include locations and applications that would previously have been completely inaccessible. The thinking networks of the future will include network nodes that are completely independent of the power grid.

Hardware for thinking networks

Like Flame, with its human data mules, thinking networks will use multiple techniques to transmit and deliver information. Single vendor solutions and proprietary data communications protocols have already become a thing of the past. Users are demanding network-wide interoperability and the ability to make use of any data communications option that may be available. Legacy serial devices are being Ethernet-enabled with Wi-Fi connections using both embeddable and external Wi-Fi Access Points. (See Fig. 2) Where a fiber optic buildout would be impractical, designers are deploying cellular routers (See Fig 3) that can establish network nodes anywhere there’s cellular telephone coverage. Thinking networks will continue the trend, using various combinations of copper cable, fiber optics, wireless and cellular data transmission. And as the network nodes get smarter, the methods used to transmit data will become increasingly irrelevant. Like Flame, thinking networks will find their way around obstacles, take advantage of whatever connection options are available, see to it that the data gets where it needs to go, and ensure that it arrives intact.

Figure 3. Cellular routers can establish network nodes anywhere there’s cellular telephone coverage.

None of this will make life any easier for network designers. Why? More and more network nodes will become independent of cable connections and the power grid. So even though network designers will be able to invest less time and energy in pursuing perfect uptime, they’ll be forced to start thinking about power budgets. Recommendations for things like 30-day battery replacement cycles will be unacceptable. Network designs will have to use power efficiently enough to ensure that remote network nodes and devices will never go dark. Traditional “always on”

communications schemes won't get the job done.

Advantages and disadvantages of thinking networks
Distributed network intelligence and integrated communications infrastructures will be engines for increased efficiency and productivity. It's estimated that 50 billion devices will be network-enabled by 2020. Many of them will be M2M devices that communicate with one another to resolve problems with no need for human intervention, much the way "smart" metering relieved utilities of the need to send employees out to visit the meters in person. Thinking networks will ultimately be able to deliver just about any data, just about anywhere, and the transmission methods involved will be completely transparent to the end user, whether that end user is a machine or a human being.

But the same hardware and software that help data travel across thinking networks will greatly complicate network security issues. Flame malware has already found a way to access the Internet from locations in which no Internet connection exists. We will soon live in a world where Internet connections are virtually everywhere.

###

Photo Credit for Figure 1 - the University of Michigan low-power, smart sensor Phoenix system:
Daeyeon Kim

Source URL (retrieved on *04/23/2014 - 6:03am*):
http://www.ecnmag.com/articles/2012/09/emergence-thinking-networks

Links:
[1] http://www.engin.umich.edu/newscenter/feature/smallsensor/