



Over the past few weeks Duqu has been getting a great deal of media attention:

Duqu: father, son or unholy ghost of Stuxnet?

Duqu virus tied to Microsoft Windows bug.

Microsoft security update addresses four flaws, not Duqu.

Duqu virus threatens virus meltdown.

Duqu underscores trouble AV industry has in stopping threats.

What is Duqu, does it represent a threat to your organization and how can you defend yourself against Duqu and similar threats?

Duqu is the latest Stuxnet like malware that has been successfully used in targeted attacks for at least several months in 2011 (maybe up to a year) before even being discovered by antivirus companies. So far it is not clear exactly what Duqu is after and whether or not it is focused on a particular industry or region.

However, if you are responsible for security for your organization Duqu is another critical reminder about what the new wave of security attacks look like - and they are quite scary. How could these organizations that had what they felt was adequate security protection in place be able to be penetrated and how could Duqu avoid detection for so long?

It was able to evade detection for so long for two reasons: It was designed to evade detection and was only used against a small group of targets. Duqu uses a driver file signed with a legitimate certificate which are generally trusted by automated scanners that are used by AV scanners. It was hidden in a WORD document and used an undisclosed Microsoft Windows security flaw. This is another example that proves that signature/reputation based AV companies are not able to protect against advanced attacks.

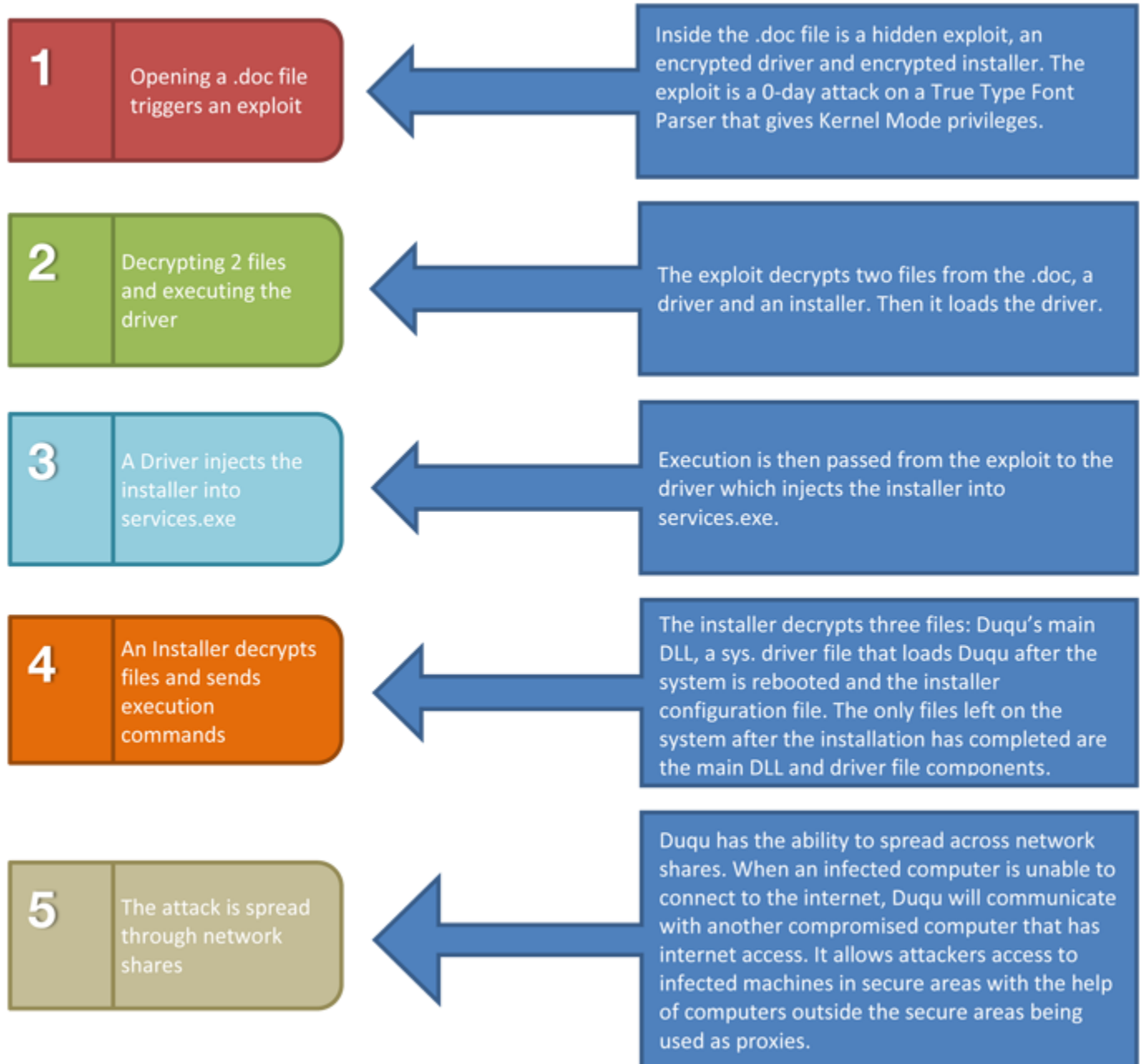
Stuxnet spread for almost a year before it was detected and Duqu possibly for as long. If the reactive techniques of AV products cannot protect you against these new attacks is there anything that you can do? In the wake of the Duqu news there are reminders to install patches, train employees, run updated malware, monitor ports, etc., etc. While these are all "best practices" that should always be employed they will not stop these attacks and neither will AV nor whitelisting.

So what is a viable defense? A security approach based on *behavioral protections*. Below is an analysis of the most current understanding of the Duqu attack and how a multi-layered behavioral protection solution like

StormShield can stop it:

The left column is a list of the steps that Duqu took in the attacks. The right column describes that attack action in more detail and, in the chart below, also defines how a security solution like StormShield can stop that attack at each step.

How the Duqu Attack worked - step by step:



How StormShield will stop this threat - step by step:



In summary:

The attackers are very smart, well funded and resourceful - they have the latest copies of the leading signature/reputation security products and know how to defeat them.

- Reactive, looking backwards security cannot stop these types of attacks. If you are relying on these you will not even know that you have been penetrated.
- Microsoft, Adobe and many other widely used applications will always have security holes that can be exploited.
- Other attackers across the world see the success of the Duqu design, are analyzing the methods used and copying them. Success begets imitation.
- A multi-layered security model and employee best practices are vital but *must* be augmented with strong behavioral

protection.

For the Duqu attack and the widely reported RSA attack before it the web discussions and blogs have been really active discussing the implications for these breaches and how they could have been prevented. Surprisingly, a significant amount of the comments fall into the category of "Oh well, I guess any system can be compromised" and "The only thing that you can do is have a good PR plan in place when the inevitable happens."

Is this true? Is there nothing that your organization can do to stop an attack like Duqu or the one that was successful at RSA? Spearphishing, APT, Zero Day and Malware are the latest vanguard of malicious attacks exploiting weaknesses in your defenses - but they can be stopped.

To better understand how this newest vanguard of attacks like Duqu work please click the link to our white paper "RSA Breach: Analysis and Protection Recommendations" to understand how RSA was breached and how you can protect your organization from this type of attack today.

Click [here](#) to download the white paper.

About Matrix Global Partners, Inc.

Headquartered in Indianapolis, Indiana Matrix Global Partners, Inc. (Matrix) is a national leader in information security solutions, integration and professional and managed services. Matrix offers a complete line of security and SIEM technologies and, as the exclusive distributor in the Americas for the award-winning StormShield security products, Matrix is growing and managing a multi-tier sales and support organization. www.MatrixGP.com.

Matrix Global Partners, Inc.

Indianapolis, Indiana

[email to: info@MatrixGP.com](mailto:info@MatrixGP.com)

Phone: (317) 514-2923