La guerre cybernétique.

Une analyse de Conficker, Stuxnet, Duqu sur la flamme, la flamme Mini, Gauss, Mahdi Shamoon

Forum pour la sécurité de l'information

www.gocs.de;-eu,-info-com.de

Version abrégée

Nous premières fois que la question simple, car a en fait déjà commencé?

Cette question peut facilement être répondu par oui et non.

Pour répondre à cette question, nous avons même pris la peine d'évaluer les communiqués de presse sur le sujet.

Pour ceux qui veulent nous accuser, nous aurions utilisé "informations zuhaltende secret". Soulignons encore une fois, nous avons seulement analysé les documents accessibles au public.

Pour la période d'analyse, nous avons utilisé seulement la période de «Stuxnet à Shamoon», c'est un temps relativement court.

Dans le même temps, une limitation en ce qui concerne les grandes masses de logiciels malveillants a été faite. Parce qu'il s'intéresse seulement les typiques "flèches" cybernétiques qui répondent à l'attribut "martial".

Mais en même temps, les structures typiques, qui sont typiques des systèmes d'armes. Mais les dépendances temporelles des systèmes d'armes individuelles.

Bien que quelques «flèches cybernétiques" ont été entièrement décrits, ils permettent un aperçu très intéressant. Où pouvez-vous regarder un, nous écrire à ce sujet plus tard, sinon ils perdent les connexions. En raison de la réalisation des pièces ne peut pas construire une stratégie de défense ou de défense. Bien sûr, cela seulement si ils le veulent.

L'ensemble de cette période devrait armes de guerre cybernétique de l'espionnage moyen de moyens de destruction sont connus pour eux, ou sont supposés connus réglé.

Nous les avons divisés en deux groupes.

Un groupe comprend les armes de destruction et de sabotage.

L'autre groupe comprend les systèmes d'espionnage, sous-systèmes, et certains, comme les systèmes de manipulation.

En vertu de cette sous-catégorie les systèmes de manipulation, les méthodes doivent être compris pour être changé lorsque les informations stockées ou supprimés. Toutefois, aucun système de contrôle de la production.

Premier Groupe

Les représentants les plus connus de ce groupe sont «Stuxnet» et «Shamoon". Leur effet est la destruction des systèmes de traitement de programme. (Stuxnet), mais aussi à la destruction de l'infrastructure informatique, tels que le stockage magnétique (disques durs), etc

La première flèche célèbre cybernétique est caractérisé par un module de destruction très spécifique. Cela ne prend que des systèmes spéciaux de contrôle de la production (systèmes d'enrichissement d'uranium avec un API de Siemens).

Lorsqu'il est utilisé contre d'autres systèmes de contrôle de la production provenant du même fabricant aucun dommage sérieux n'a été observé.

La première utilisation de cette flèches cybernétiques se caractérise par une particularité. Ce sont les premières attaques de l'utilisation sélective - c'est - à travers une mise en œuvre directe dans le système cybernétique réalisé (ordinateur). Selon divers articles de presse les deux attaques ont été menées par des employés autorisés des centres informatiques respectifs.

Cette lié aux attentats en Iran, ainsi que les attaques en Arabie Saoudite, où l'industrie pétrolière a été touché.

Mesure dans laquelle les mesures de sécurité internes qui ont réduit leurs pertes, n'est pas connue.

Pourrait donc aucun agent de conservation du système de communication (Internet ou autres moyens de communication) ne sont pas efficaces. Dans une telle attaque mesures de sécurité sur Internet ne sont pas efficaces (que l'on appelle le siège de la défense cybernétique).

Cela était vrai pour l'utilisation de «Stuxnet» et «Shamoon" semblables.

Combien de ces infections ont été effectuées par des employés autorisés est inconnue. Pour ce type d'attaque n'est que d'une importance qui a eu lieu ce directement dans le système informatique.

Ce type est le type qui nécessite un système de protection directement dans le système informatique ou systèmes d'exploitation correspondants et les mesures de protection plus strictes, comme l'encodage interne ou le chiffrement. Des systèmes de protection connus de l'autre. Cela ne signifie rien, ces systèmes doit être fondé sur la valeur de l'information.

Dans le cas de «Stuxnet» a eu lieu après la première utilisation, même pour une infection massive par le biais de l'Internet. Il aurait été infecté environ 60.000 unités. Quel devrait être le but de cette distribution n'est pas claire, comme «Stuxnet» une flèche hautement spécialisé cybernétique a été et est toujours.

Les trous puis dans les systèmes logiciels ont été utilisés qu'après une longue période, rempli plusieurs mois.

A été réalisée à cette «Flickenschusterei», une guerre cybernétique (cyberguerre) aurait pu être réalisée avec succès sur ces trous.

Le pénétrateur permis une intrusion très intelligent. Le successeur ou les produits de la plateforme mêmes utilisent une variété de pénétrateurs.

Combien d'autres trous que là-bas!

L'accent, même dans les résultats actuels, du fait que seuls les modules nuisibles doivent être remplacés par d'autres caractéristiques de la cible.

Le même comportement s'applique également à la «pénétration» de pénétrer dans les unités respectives cybernétiques (systèmes informatiques).

La modularité est une caractéristique des flèches modernes cybernétiques.

Deuxième Ce deuxième groupe est beaucoup plus vaste. Connu représentants Duqu, Flamme, Gauss, Mini flamme et Mahdi.

Ce groupe peut être décrit comme «espions cybernétiques". Cette espions cybernétiques sont marqués par les caractéristiques classiques d'espions.

C'est spécial et la cybernétique intelligence plus en détail.

Le groupe d'espions cybernétiques a été utilisé de manière très différente. Le Duqu représentants et Mahdi ont institué que dans un petit nombre. Cela signifie rien de plus que le nombre relativement faible de ces flèches cybernétiques ont été utilisés et ce qui peut être le cas, il y avait très peu découvert. Également sur les missions spéciales de ce qui signifie peu connu. Néanmoins, ils sont considérés comme "très dangereux". Dim., entre autres, également sur la BSI / Allemagne. Provenant d'autres sources, utilisation à long terme n'est pas exclue avec les modules d'espionnage nouvelles.

Il peut être comparé à un des satellites de reconnaissance Duqu. Il est là, mais un autre ne sait pas!

Il doit être assumée par ces sources avec une utilisation renouvelée. Selon les expériences connues de la mise au point d'une variété de plates-formes, "Duqu et Stuxnet" systèmes les plus avancés sont utilisés.

Même cette ligne de développement est évident dans les systèmes d'espionnage connus.

Il trouve également la plate-forme - l'application principe. Cela ne signifie rien, les systèmes ont fait leurs preuves sont développées grâce à l'utilisation de nouveaux modules pour le type de tâche. Dans le même temps, l'expérience peut être modifié avec les anciennes solutions et optimisé pour répondre aux exigences croissantes. L'analyse porte sur les modules ainsi que les modules de communication. Ce dernier point est particulièrement important car ils ont gagné doit passer des informations aux serveurs cachés. Cela s'applique à la quantité d'informations ainsi que pour le

secret. Pour cette raison, l '«information récupérée" transmis sous forme cryptée ou cryptés. Le même principe a été utilisé dans la seconde guerre mondiale. Ainsi, les informations obtenues à partir de la "Enigma", codé pour la transmission. Quelle est la procédure utilisée du côté britannique est venu semble être encore un mystère. Tout ce processus a reçu le nom "Ultra".

Cela a empêché que le côté allemand prend connaissance de "l'effondrement" dans le système de cryptage Enigma tandis que l'information décryptée est protégé. Il a également donné une analogie dans les années quatre-vingt dans le contexte de l'information décryptée par la ZCO ex.DDR.

Cette ancienne méthode est détectable même en les espions cybernétiques. Encore une fois, l'information est protégée, il n'y a donc pas de vision de l'espionnage d'informations possible. En outre, en ce qui concerne ces informations, qui se transmet de la transmission aux serveurs, pas un guide pour les "informations intéressantes."

L'objet cybernétique, qui a été élucidée par ces flèches cybernétiques devriez obtenir aucune preuve significative que les informations pour l'élucidation d'importance.

Encore une fois, il s'agit d'une approche très intéressante:

(1)

Certains acheteurs acheter des «supports magnétiques" avec des informations intéressantes et utiles pour eux (données fiscales, par exemple pour les fraudeurs fiscaux allemands) et payer des millions €. La valeur de cette information est un multiple.

Sur le marché de l'information est généralement connu, les autorités financières européennes à la recherche "d'informations à propos de la multiplication de l'argent".

Comme ces informations ne seront pas vendus sur le marché, ils seront disponibles seulement pour les «illégalement». Ces actes sont effectués par des «personnes autorisées».

(2)

Une autre forme d'acquisition d'information, qui nécessite l'utilisation d'un agent cybernétique est préféré par les autres.

Dans ce cas, assumer la fonction du collecteur flèches informations cybernétique dans d'étranges systèmes cybernétiques. Les informations recueillies seront transmises via le serveur de communication. Dans certains cas, les données doivent être transmises par la taille de 5 gigaoctets massif. Toutefois, ils peuvent être plus ou moins.

La collecte de données par l'intermédiaire de "flèche cybernétique» est plus souple par rapport à une source humaine. L'utilisation de ces flèches permet de donner une réponse au client ajustement idéal correspondant.

Il s'ensuit, bien sûr, un avantage que vous pouvez apporter des changements rapides, car le principal, a découvert un autre sources inconnues.

Parmi les caractéristiques de l'intelligence cybernétique sans doute entendu parler de la variabilité rapide dans la cible.

Les différentes approches sont tributaires des formes de gouvernement.

Ceux-ci ont Spionagehelferlein petite, comme tout autre programme ou la taille Flèche cybernétique. Certains d'entre eux mince, tandis que d'autres sont de gros bateaux. Ils proviennent d'une même plate-forme.

Le plus connu «grand bateau» est «la flamme».

L'utilisation d'espions cybernétiques est très différente.

Donc, d'une façon ou Duqu ou flamme Mini être utilisé en petites quantités. Il est prévu pour chaque système avec jusqu'à 60 infections.

Le nombre total de ces espions spéciaux cybernétiques est donc d'environ 120 infections.

Il semble ici être un espion hautement spécifique et sensible cybernétique.

L'information disponible pour l'analyse ne peut pas être évaluée.

D'autres, cependant, être utilisé avec modération. Alors que les taux d'infection ont été trouvés dans 10.000 ou plus.

Infections flamme d'environ 5.000 à 6.000

Gauss environ 2.500 infections

Mahdi supérieure à 700 infections

Conficker environ 60.000 ou peut-être même plus.

Les taux d'application de ces espions cybernétiques ont augmenté de 10 fois à 100 fois au cours des régimes spéciaux. Dans certains cas, cette valeur peut être dépassée de manière significative (Conficker).

La zone d'infection varie d'un minimum de 68 200 et un maximum de 100.000 ou plusieurs infections.

Le chiffre réel est beaucoup plus élevé. De l'analyse des autres systèmes nuisibles peuvent être assumées par des facteurs entre 3 ... 8.

Les raisons du nombre élevé de cas inconnus sont connus et ne seront pas examinées plus avant.

Sur la répartition géographique des «programmes malveillants trouvés» pour être traité ici volontairement indéterminée. Depuis un certain nombre d'applications de flèches cybernétiques

fournit d'autres résultats différents. Dans le même temps, l'utilisation de certaines flèches cybernétiques dans une géopolitique est illogique.

Un point très intéressant est l'analyse Fragegestellung dans quels domaines, de la politique, de l'économie, de l'armée, de la recherche et du développement, de l'infrastructure et si dévoués

Leurs résultats sont très intéressants.

Ces résultats ne sont pas publiés comme «mauvaises interprétations» entre les banaliser et alarmiste d'une guerre cybernétique pourrait conduire à des scénarios apocalyptiques.

Une analyse préalable 10.12.2012

Notes:

Ce matériel fait partie du "Forum pour la sécurité de l'information».

Il est publié et mis à jour en permanence.

Ce matériel est basé uniquement sur les publications disponibles au public.

Publié sur Internet aux adresses suivantes:

www.gocs.de ou www.gocs.eu ou www.gocs.info ou www.gocs.com.de

23.12.2012 Berlin,

GOCS Auteur Vieux

Réutilisées avec l'autorisation de l'auteur. Cette analyse sera mise à jour continuellement. Sous réserve d'erreurs.