Категории вредоносных объектов, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям. Для того чтобы дать лучшее представление о типах заблокированных угроз, мы выполнили их детальную классификацию.

- **Ресурсы в интернете из списка запрещённых.**

  Веб-антивирус защищает компьютер, когда установленные на нем программы (браузеры, почтовые клиенты, компоненты автообновления прикладного ПО и др.) пытаются подключиться к IP и URL адресам, занесенным в список запрещённых. Такие ресурсы связаны с распространением или управлением каким-либо вредоносным ПО.

  В частности, в списки запрещённых попадают также ресурсы, на которых распространяется, например, вредоносное ПО типа Trojan-Spy и Ransomware, замаскированное под утилиты для взлома/сброса пароля на контроллерах различных производителей, crack/patch для промышленного и инженерного программного обеспечения, используемого в технологической сети.

- **Вредоносные скрипты и фишинговые страницы (JS и HTML).**
- **Эксплойты для браузеров.**
- **Троянцы-шпионы, бэкдоры и кейлоггеры,**

  которые встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Как правило, конечная цель таких атак — кража денег.

- **Вредоносные документы (MSOffice+PDF),**

  содержащие эксплойты, зловредные макросы и зловредные ссылки.

- **Программы-вымогатели.**
- **Черви (Worm)**,

распространяющиеся, как правило, через съемные носители и сетевые папки, а также черви, распространяющие через почтовые сообщения (Email-Worm), сетевые уязвимости (Net-Worm) и мессенджеры (IM-Worm). Большинство червей являются устаревшими с точки зрения сетевой инфраструктуры управления ими. Но есть среди них и такие как Zombaque — с реализованной P2P сетевой архитектурой, позволяющей злоумышленникам активировать его в любой момент.

- **Вредоносные программы класса Virus.**

  Среди этих программ уже много лет детектируются такие семейства как Sality, Nimnul, Virut. Хотя эти вредоносные семейства считаются устаревшими, поскольку их командные серверы управления давно не активны, они традиционно вносят значительный вклад в статистику в силу самораспространения и недостаточных мер по их полному обезвреживанию.

- **Вредоносные LNK-файлы.**

  Такие файлы, в основном, блокируются на съемных носителях. Они являются частью механизма распространения для таких старых семейств вредоносного ПО как Andromeda/Gamarue, Dorkbot, Jenxcus/Dinihou и других.

  В этой категории также широко представлены LNK-файлы с уязвимостью CVE-2010-2568, которая впервые была использована для распространения червя Stuxnet, а затем стала использоваться для распространения множества семейств, таких как Sality, Nimnul/Ramnit, ZeuS, Vobfus и других.

  В настоящее время замаскированные под легитимный документ LNK-файлы могут использоваться как часть многоступенчатой атаки. Они запускают powershell-скрипт, скачивающий зловредный файл.

  В редких случаях запускаемый вредоносный powershell скрипт скачивает и внедряет в память бинарный код, являющийся специфичной модификацией пассивного TCP бэкдора из набора metasploit.

- **Вредоносные файлы (исполняемые, скрипты, autorun.inf, .LNK и другие), которые запускаются автоматически при запуске системы или при подключении съемного носителя.**

  Это файлы из множества разнообразных семейств, которые объединены фактом автозапуска. Из наиболее «безобидной» функциональности у подобных файлов — автоматический запуск браузера с предустановленной стартовой страницей. В большинстве случаев вредоносное ПО,

использующее autorun.inf, является модификацией зловредов старых семейств (Palevo, Sality, Kido и др.).

- **Вредоносные программы для AutoCad.**

  Отметим, что вредоносное ПО для AutoCad, в частности вирусы, детектируются преимущественно в Восточной Азии — на компьютерах технологических сетей, в том числе в сетевых папках и на рабочих станциях инженеров.

- **Майнеры — исполняемые файлы для ОС Windows**
- **Веб-майнеры, выполняемые в браузерах.**
- **Банковские троянцы.**
- **Вредоносные файлы для мобильных устройств,**

  которые блокируются при подключении устройств к компьютерам.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com